MANUAL DO FORNECEDOR DE TI

TUPY

Revisão: Junho/2024

Tecnologia de Informações

TUPY

Sumário

1. OBJETIVO DO MANUAL

Este manual tem por objetivo atender os procedimentos internos da área de TI (“TI”) da Tupy, assim como, adequar as responsabilidades necessárias para a execução dos serviços ora contratados, a EMPRESA deve se comprometer a:

- Cumprir as normas contidas na Norma da Segurança da Informação e Cibernética (“NSI”) (ref. NCT061);
- Solicitar aprovação junto à área de TI antes de executar qualquer mudança no ambiente da Tupy, seja em sistema ou no ambiente físico, conforme processo de gerenciamento de mudanças de TI (ref. IT029);
- Manter informado seus profissionais internos, dos procedimentos estabelecidos pela Tupy;
- Cumprir com todos os procedimentos operacionais de TI em caso de atendimento de incidentes (ref. IT039 e IT056);
- Sempre solicitar à TI as definições de Arquitetura aplicáveis para as respectivas plataformas de desenvolvimento no caso de desenvolvimentos de sistemas, devendo cumprir com as todas as determinações;
- Utilizar o ambiente da Tupy exclusivamente para a realização dos serviços contratados;
- Utilizar somente sistemas licenciados na execução dos serviços contratados pela Tupy;
- Manter confidencialidade sobre todas as informações que, por qualquer meio (direto ou indireto), tenha conhecimento, em razão dos serviços ora contratados;
- Comunicar imediatamente a Tupy, sobre o desligamento de seus profissionais internos;
- Prezar pela segurança da informação de seu ambiente, minimizando possíveis impactos para a Tupy;

Além deste Manual, a EMPRESA deverá observar as disposições previstas nas Condições Gerais de Fornecimento Tupy, disponível através deste link.

Para obter informações detalhadas sobre os processos citados neste documento, buscar a área de Governança de TI através do e-mail segurancadainformacao@tupy.com

2. PROCESSOS DE TI

2.1. Norma da Segurança da Informação e Cibernética (NCT061)

O objetivo desta norma é preservar a segurança das informações, de acordo com a sensibilidade dos dados e das informações sob responsabilidade e de titularidade da Tupy, o que inclui a integridade, disponibilidade e confidencialidade dessas informações; e regular a utilização adequada dos recursos de TI disponibilizados para execução das atividades em nome da Tupy, incluindo equipamentos eletrônicos, Internet, endereço eletrônico, dentre outros, conforme definido na NSI.

As diretrizes abaixo serão objeto de procedimentos específicos, quando for o caso.

- **Informações Tupy:** É proibido acessar, copiar, transferir, encaminhar para dispositivos e/ou repositórios pessoais (incluindo, mas não se limitando a celular, pen drive, HD externo, caixas de e-mail, Dropbox etc.), modificar, destruir ou divulgar a Funcionários e/ou Terceiros, qualquer informação de titularidade da Tupy ou de titularidade de outra entidade que tenha eventualmente disponibilizado sua informação à Tupy, sem a competente autorização prévia e expressa do respectivo titular.
- **Dados Pessoais:** É proibido realizar o Tratamento de qualquer Dado Pessoal e/ou Dado Pessoal Sensível de Funcionários, e seus familiares Terceiros, clientes e fornecedores, sem amparo em uma das bases legais definidas pela LGPD ou sem a autorização do seu titular ou responsável (no caso de menor de idade), conforme aplicável.
- **Inteligência Artificial (IA):** É expressamente proibido utilizar "Informações Tupy" (exemplos: informações confidenciais, propriedade intelectual, segredos comerciais e industriais, projetos e informações estratégicas) e/ou "Dados Pessoais" em sites/aplicativos públicos de inteligência artificial (IA), tais como por exemplo CHATGPT, entre outros. A utilização destes sites/aplicativos de forma indevida, é passível de aplicação das medidas legais e disciplinares cabíveis.
- **Divulgação da marca ou nome da Tupy,** de forma ilegal em páginas da Internet, é passível de aplicação das medidas legais e disciplinares cabíveis.
- **Gestão de Acessos**: Todos os acessos aos sistemas informatizados da Tupy devem ser revogados ou bloqueados nas seguintes condições: desligamento ou afastamento do funcionário, estagiário ou aprendiz da empresa, desligamento ou afastamento do terceiro na empresa contratada ou na Tupy.
- **Acesso Remoto:** A concessão de uso do recurso de acesso remoto deve ser realizada mediante abertura de chamado na Central TI, contendo prazo de início e término e aprovação do gestor.
- **Login e Senha:** A Identidade de Acesso do usuário de TI ("Login") e Chave de Acesso ("Senha") são pessoais e intransferíveis.
- É proibida a utilização da Identidade de Acesso do usuário de TI ("Login") e Chave de Acesso ("Senha") por qualquer outra pessoa que não seu titular.

- O usuário deve alterar a sua Chave de Acesso (“Senha”) sempre que solicitado pela área de TI, conforme regras estabelecidas.
- **Mensagens Eletrônicas (E-mail):** O Usuário reconhece que os dados enviados, recebidos, ou de qualquer forma transmitidos pelo correio eletrônico da Tupy não são considerados particulares ou da esfera privativa do Usuário, na medida em que disponibilizados exclusivamente para a atividade profissional, pelo que não deve esperar privacidade ao utilizar esse meio de comunicação.
- **Boas Práticas:** O Usuário não deve realizar ou contribuir para a corrupção de informações ou dados de propriedade da Tupy ou de terceiros, bem como não deve violar direitos de propriedade intelectual da Tupy, de seus clientes ou de terceiros, seja através de cópia, impressão, distribuição ou qualquer outro meio não autorizado pelo titular da informação.
- **Gestão de Mudanças**: Antes de executar qualquer mudança no ambiente da Tupy, tanto em sistemas quanto no ambiente físico, o usuário se compromete a buscar a aprovação junto a área de TI, conforme o processo de gerenciamento de mudanças estabelecido.
- **Auditoria:** A Tupy monitora e audita a utilização dos recursos de TI pelos usuários, sempre que entender necessário, zelando pelo cumprimento destas diretrizes.

O descumprimento de qualquer das diretrizes da NSI é motivo de aplicação das medidas legais e disciplinares que a Tupy entender cabíveis, podendo o usuário infrator responder civil e criminalmente.

2.2. Gestão de Mudanças de TI (IT029)

O Processo “Gerenciar Mudanças de TI” tem por objetivo padronizar as tratativas para as mudanças, garantindo que as mudanças tenham seus riscos devidamente avaliados, visando minimizar impactos negativos no ambiente de TI.

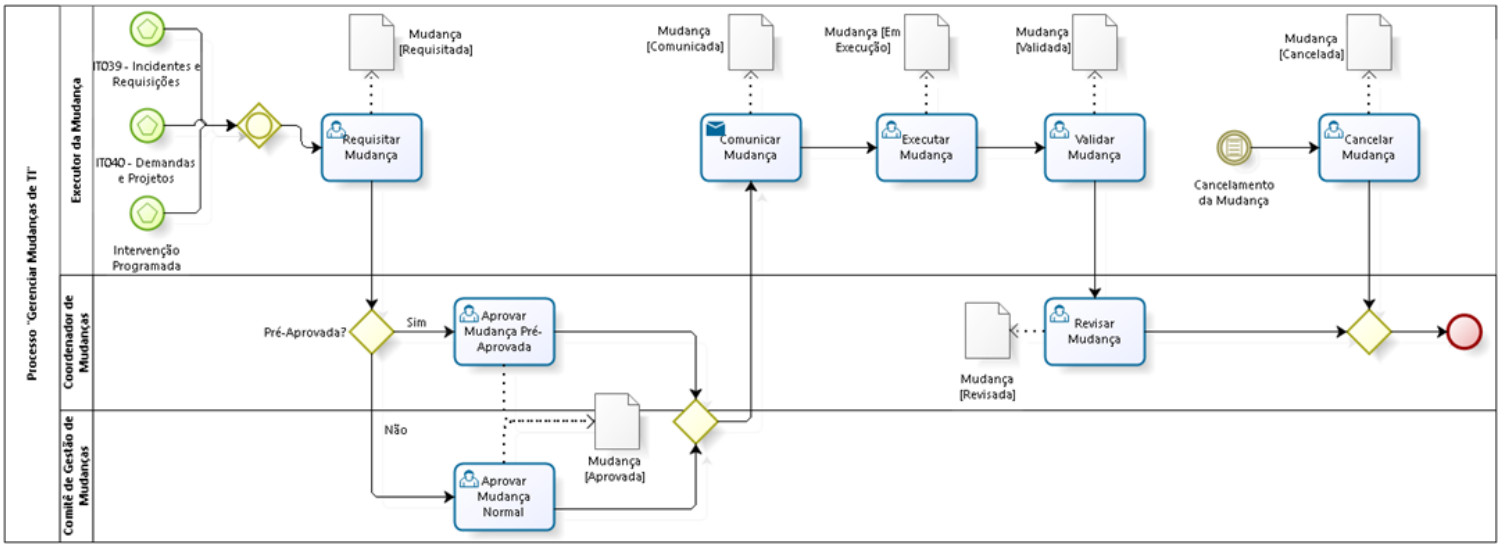

Figura: Processo Gerenciar Mudanças de TI

2.2.1. Regras de Aprovação e Comunicação de Mudanças

Classificação		Aprovação		Comunicação	
Tipo	**Urgência**	**Responsável**	**Considerações**	**Antecedência**	**Público**
Pré-Aprovada	Não emergencial	Coordenador de Mudanças	A Mudança deve seguir o calendário de liberação dos IC’s afetados	1h	TI
Pré-Aprovada	Emergencial	Coordenador de Mudanças	O Coordenador de Mudanças deve solicitar antecipação de janelas de liberação dos IC’s afetados (quando aplicável)	Livre	TI *
Normal	Não emergencial	Comitê de Gestão de Mudanças	A aprovação deve ser realizada em reuniões ordinárias do Comitê	Mínimo de 1h (validar com o comitê)	TI e áreas impactadas
Normal	Emergencial	Comitê de Gestão de Mudanças ou Gerente Responsável	O Coordenador de Mudanças deve solicitar uma reunião extraordinária do Comitê ou solicitar aprovação ao Gerente de TI responsável	Livre	TI e áreas impactadas *

* Quando uma mudança for classificada como emergencial é necessário incluir uma informação de que se trata de uma mudança emergencial no comunicado enviado.

2.3. Gestão de Atendimento de Serviços de TI (IT039)

Os Incidentes de TI são tratados de forma estruturada através das etapas de Identificação, Avaliação, Atendimento e Encerramento de um Incidente de TI à medida em que eles ocorrem, agilizando e minimizando os impactos para a organização e/ou componentes de TI.

O Desastre de TI é o último nível de criticidade de um Incidente de TI, conforme progressão abaixo.

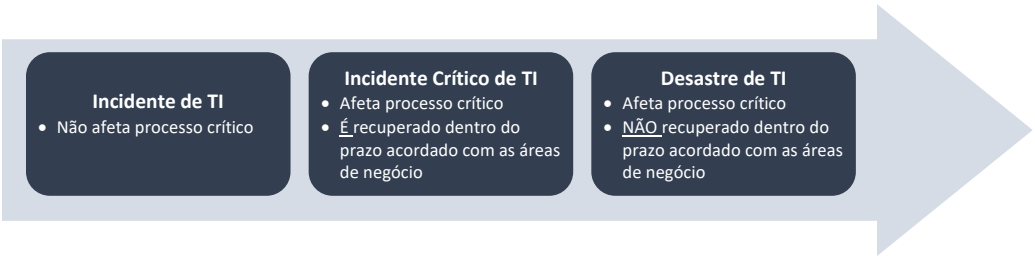

Figura: “Criticidade dos Incidentes de TI”

Chamados com mesma escala de criticidade, pontualmente podem ter prioridades distintas. Cada caso de priorização deve ser tratado diretamente com o líder de suporte da equipe responsável pelo atendimento.
Algumas estações de trabalho da área fabril estão cadastradas como críticas, e independente do horário os chamados são tratados como críticos, automaticamente com criticidade “muito alto”.
A equipe da Central de Serviços (ramal 8585) atua em regime de plantão entre 01:00 h e 07:00 h de terça à sexta-feira e das 01 horas de sábado às 7 horas de segunda-feira.
Em casos específicos, a análise pode precisar de apoio de equipe de suporte N4. Este nível de suporte geralmente é representado pelo fabricante do sistema ou componente de infraestrutura que o chamado está tratando. É de responsabilidade da TI da Tupy abrir uma solicitação em ferramenta distinta de chamados e fazer o acompanhamento até a sua resolução. Da mesma forma, que é responsável por facilitar as interações entre as equipes e solicitante interno.
Chamados que resultem em alterações no ambiente obedecem a critérios específicos à gestão de mudanças, envolvendo o teste adequado no ambiente destinado a este fim, aprovações/evidências pós testes e respeito as janelas de atualizações às terças e quintas-feiras, sempre às 14 horas, salvo exceções. Os chamados em que sua proposta de solução envolva alteração crítica em ambiente produtivo, com possibilidade de impacto mais amplo ao item tratado deve passar pelo comitê de mudanças de TI. As alterações exigem de TI, um comunicado de mudança aos envolvidos. Vide IT029.

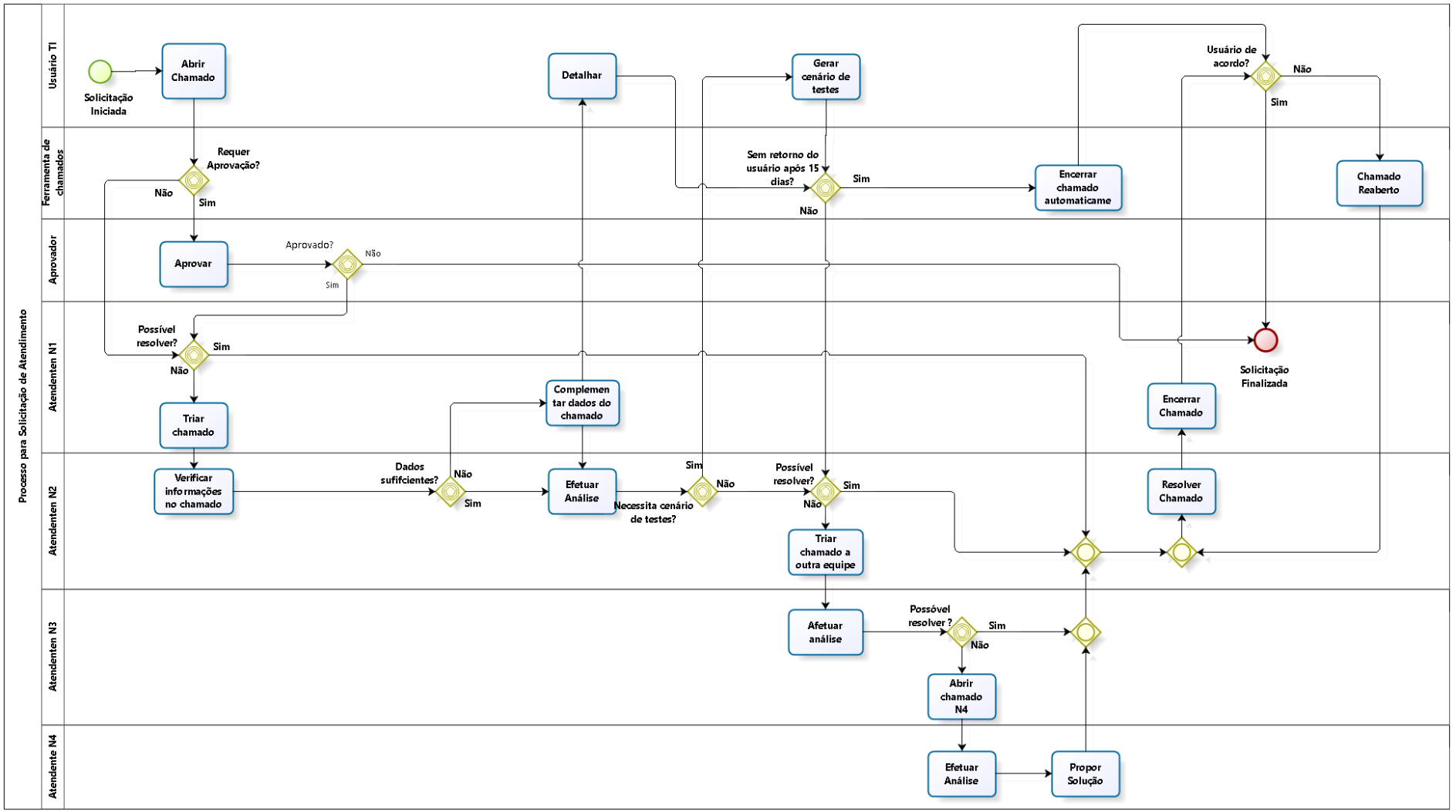

Figura: Processo para Solicitação de Atendimento

2.4. Plano de Respostas a Incidentes (IT056)

O “Plano de Resposta a Incidentes de TI” permite gerenciar incidentes de forma estruturada através das etapas de Identificação, Avaliação, Atendimento e Encerramento de um incidente de TI à medida em que eles ocorrem, agilizando e minimizando os impactos para a organização e/ou componentes de TI.

2.4.1. Processo “Tratar Incidentes de TI”

O objetivo deste processo é definir e formalizar as atividades que devem ser executadas para o tratamento dos incidentes de TI, registrados através da ferramenta de chamados da área de TI.

Incidente de TI: Evento de redução, parcial ou total, dos níveis de atendimento, que pode impactar a disponibilidade, integridade ou confidencialidade de um serviço de TI.

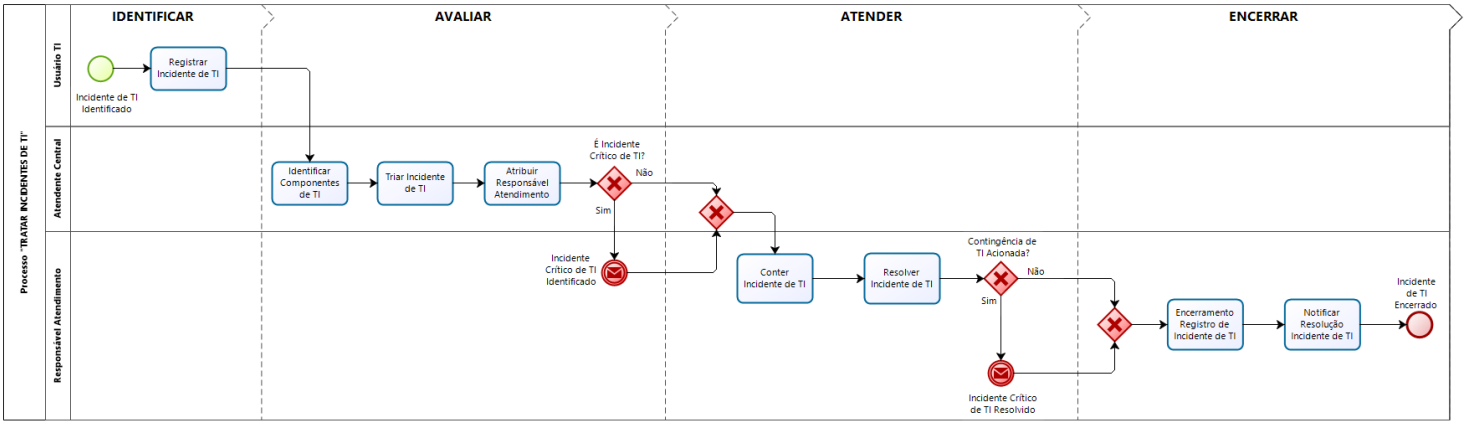

Figura: Processo “Tratar Incidentes de TI”

2.4.2. Processo “Tratar Incidentes Críticos de TI”

O objetivo deste processo é definir e formalizar as atividades necessárias para minimizar os impactos causados por um incidente crítico de TI, e permitir o restabelecimento dos componentes o mais rápido possível.

Incidente Crítico de TI: Quando um Incidente de TI passa a afetar um processo crítico do negócio (v. BIA), o mesmo torna-se um Incidente Crítico de TI. Um processo crítico é afetado quando a capacidade de controlar seu impacto é perdida.

Em um Incidente Crítico de TI a extensão do dano é recuperada dentro do prazo acordado com as áreas de negócio. Quando o dano não é recuperado dentro do prazo acordado, o mesmo torna-se um Desastre de TI.

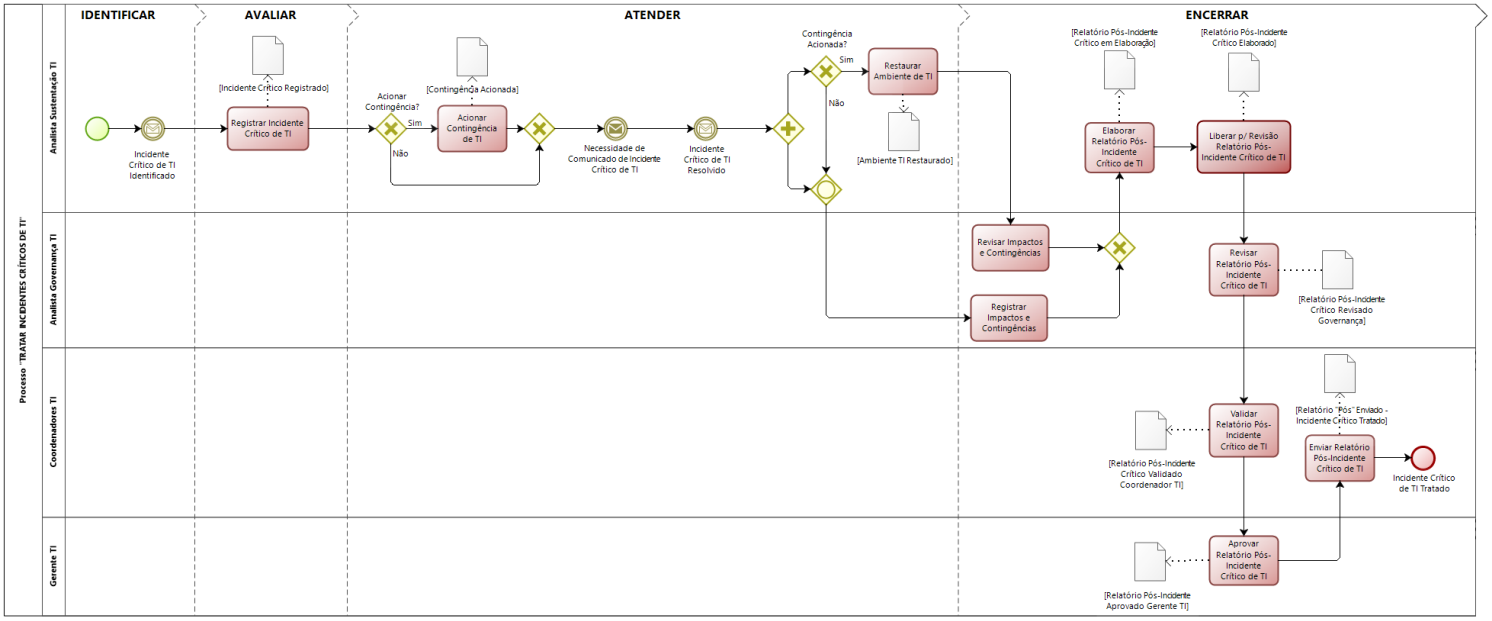

Figura: Processo "Trata Incidentes Críticos de TI"

2.5. Plano de Recuperação de Desastre de TI (IT060)

O “Plano de Recuperação de Desastre de TI” permite o restabelecimento dos processos críticos à normalidade, em decorrência de um serviço de TI interrompido, após prazo superior ao acordado com as áreas de negócio.

O “Plano de Recuperação de Desastre de TI” tem como objetivos:

- Estabelecer prioridades e respostas mais adequadas aos cenários de desastre de TI;
- Facilitar a coordenação e comunicação com a alta gestão e demais partes envolvidas;
- Assegurar a prontidão da organização para suportar um desastre de TI;
- Reduzir o impacto financeiro, operacional, legal e de imagem, decorrente de um desastre de TI.

Os processos operacionais que forem interrompidos, em decorrência de um “Desastre de TI”, deverão seguir os planos de contingências específicos, de cada área de negócio, para serem restabelecidos.

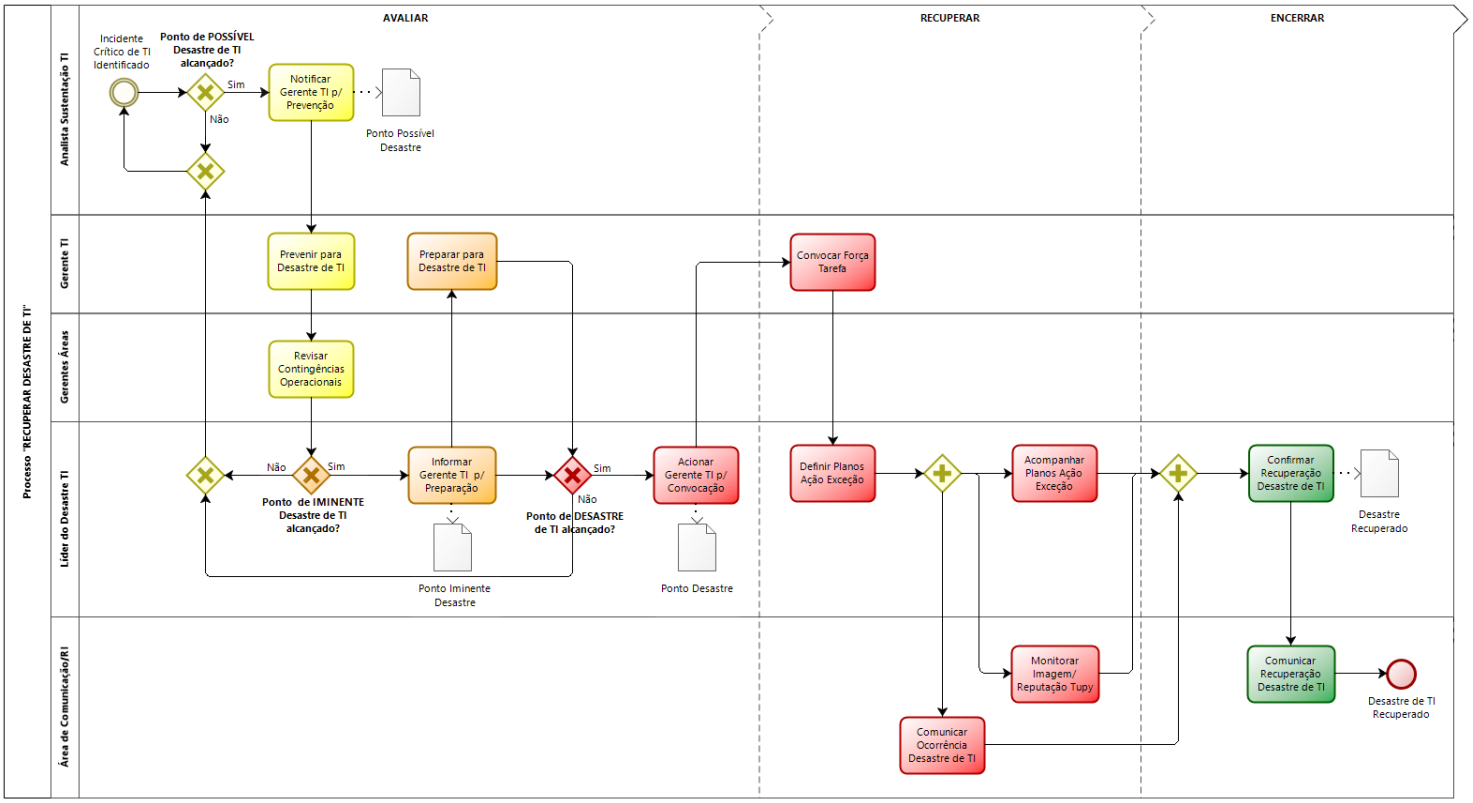

Figura: Processo “Recuperar Desastre de TI”

2.5.1. Nível de Acionamento de Desastre de TI

Para antecipar as ações necessárias frente à possibilidade de ocorrência de um Desastre de TI, foram estabelecidos os pontos de acionamento abaixo, que de acordo com o nível atingido disparam ações específicas no processo.

Ponto de **POSSÍVEL** Desastre de TI	Ponto onde é identificado que um Incidente Crítico de TI poderá se tornar um Desastre de TI.
Ponto de **IMINENTE** Desastre de TI	Ponto onde é identificado que um Incidente Crítico de TI está próximo de se tornar um Desastre de TI.
Ponto de **DESASTRE** de TI	Ponto onde é identificado que um Incidente Crítico de TI se tornou um Desastre de TI.

Todo evento crítico de TI definido para os processos de negócio da Tupy, possui limites de horas estabelecidos para o alcance de cada ponto de acionamento de Desastre de TI.
Os eventos críticos de TI relativos à Segurança da Informação, não possuem limites de horas estabelecidos para o alcance de cada ponto de acionamento de Desastre de TI, sendo tratados como exceção.

Evento Crítico de TI - BR	Ponto de POSSÍVEL Desastre de TI	Ponto de IMINENTE Desastre de TI	Ponto de DESASTRE de TI
Segurança da Informação - Sequestro das informações da empresa causado por pessoa mal intencionada	Suspeita, tratar como incidente critico	Tratar suspeita com análise forense	Suspeita confirmada! Desastre de TI
Segurança da Informação - Vazamento das informações de clientes, atingindo a reputação e imagem da Tupy			
Segurança da Informação - Vazamento das informações do processo de produção para a concorrência			
Segurança da Informação - Vazamento de informações "Pessoais" (funcionários, clientes, fornecedores, etc.) sob controle da Tupy			
Segurança da Informação - Utilização indevida dos recursos tecnólogicos para fins não autorizados.			