Secretaria de TIC do TRT24

GESLAINE PEREZ MAQUERT
16/05/2023 15:43

Processo Gerenciar Controle de Acessos

Histórico do Documento

	Data	Descrição
01	12/11/2015	Desenho do processo
02	19/04/2016	Descrição do processo
03	17/08/2018	Alinhamento COBIT 5.0 e merge das atividades de gerenciamento de acessos lógicos e físicos
04	11/04/2023	Primeira revisão para melhoria do processo

Secretaria de TIC do TRT da 24ª Região

Documento de Descrição de Processo de Trabalho

Processo Gerenciar Controle de Acessos

11/04/2023

Equipe de Documentação

	Nome	Cargo
01	Geslaine Peres Marquete	Chefe da Divisão de Proteção de Dados e Segurança da Informação
02	Fábio Nogueira da Silva	Membro da equipe da Divisão de Proteção de Dados e Segurança da Informação

Sumário

1. Objetivo

Descrever as atividades, fluxos de trabalho, responsáveis e responsabilidades relativas ao gerenciamento do controle de acessos lógicos e físicos, em alinhamento à Política de Segurança da Informação do TRT da 24ª Região e aos instrumentos normativos que a compõe.

2. Abrangência

Secretaria de Tecnologia da Informação e Comunicações (SETIC).

3. Definições

- **Acesso lógico:** qualquer tipo de contato entre o usuário de TIC e as informações armazenadas em sistemas, aplicativos, ferramentas, sistema operacional ou outros ativos de TIC do TRT da 24ª Região;
- **Acesso físico**: qualquer forma de contato físico entre o usuário de TIC ou um prestador de serviços e qualquer tipo de equipamento de armazenamento de dados;
- **Ativos de TIC** - qualquer mecanismo ou dispositivo de software ou hardware que compõem a infraestrutura da rede de dados do TRT24 e que é utilizado como ferramenta de trabalho para o desempenho funcional dos magistrados e servidores do Tribunal;
- **Conta de usuário de TIC:** identificação pessoal e intransferível formada por login e senha, criada automaticamente no momento do cadastro no Sistema de Recursos Humanos e que permite acesso à rede de dados, intranet, email, sistemas e demais recursos de TIC oferecidos pelo TRT24;
- **Controle de acesso:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;
- **Manual de Controle de Acessos:** documento integrante da Política de Controle de Acessos que descreve os aspectos técnicos relativos ao controle de acessos lógicos e físicos;
- **Perímetro crítico**: ambiente destinado a armazenar ativos de TIC, cuja interrupção não programada do funcionamento ou a indisponibilidade comprometem significativamente as atividades do TRT24;
- **Prestador de serviço**: pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso;
- **Sala Cofre:** ambiente crítico destinado a proteger os ativos de TIC mais importantes contra ameaças naturais (calor, umidade, fogo, etc.) e intencionais (acesso indevido, roubo, arrombamento, sabotagem, etc.);
- **Sala Técnica:** perímetro crítico das unidades do interior do estado e prédios da capital;
- **Termo de Adesão à Política de Segurança da Informação:** documento integrante da Política de Controle de Acessos onde o usuário de TIC declara conhecer e aderir as normas estabelecidas pela Política de Segurança da Informação do TRT24;
- **Usuário de TIC**: todos aqueles que exerçam, ainda que transitoriamente e sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública em qualquer unidade organizacional do TRT da 24ª Região.

4. Processo Gerenciar Controle de Acessos

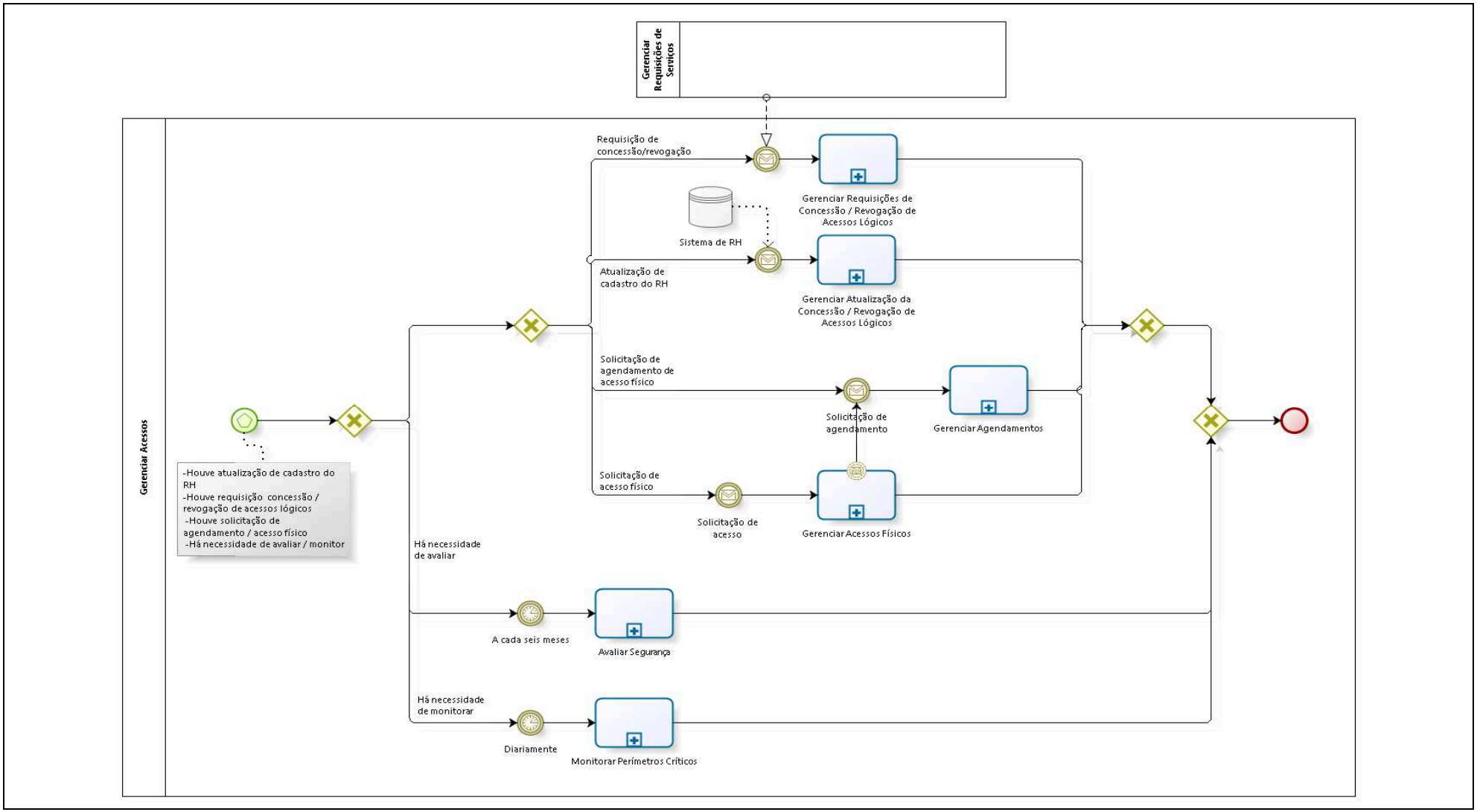
4.1. Papéis e Responsabilidades

Papel	Responsabilidades	Responsável
Dono do Processo	• Assegurar que todos os envolvidos na execução do processo sejam informados das mudanças e suporte efetuados • Aprovar as atualizações do processo • Buscar a qualidade e eficiência gerais do processo	Secretário de Tecnologia da Informação e Comunicações
Gerente do Processo	• Buscar a eficiência e a efetividade do processo • Manter o desenho e indicadores do processo atualizados, garantindo que estejam adequados aos propósitos da organização • Produzir informações gerenciais (indicadores) • Promover a execução das atividades do processo	Chefe da Divisão de Proteção de Dados e Segurança da Informação
Gerente de Segurança	• Definir e manter atualizados os perímetros críticos • Garantir que os mecanismos automatizados de concessão/revogação de direitos estejam em funcionamento adequadamente • Oferecer suporte aos gestores de sistemas para garantir que os direitos de acessos estejam alinhados a atribuição atual dos usuários de TIC • Promover a assinatura dos Termos de Adesão • Registrar solicitações de acessos • Registrar agendamento de acessos • Realizar ou promover continuamente testes de segurança nos dispositivos de segurança dos perímetros críticos • Reportar ao Comitê de Segurança da Informação e Proteção de Dados os eventos relacionados a quebras de segurança ou desconformidades • Tomar as providências cabíveis em casos de ocorrência de incidentes de segurança da informação	Chefe da Divisão de Proteção de Dados e Segurança da Informação
Responsável pelo perímetro	• Autenticar acessos físicos • Comunicar acessos físicos ao Setor de Segurança da Informação • Negar / interromper acessos físicos • Permitir acessos físicos	Servidor designado

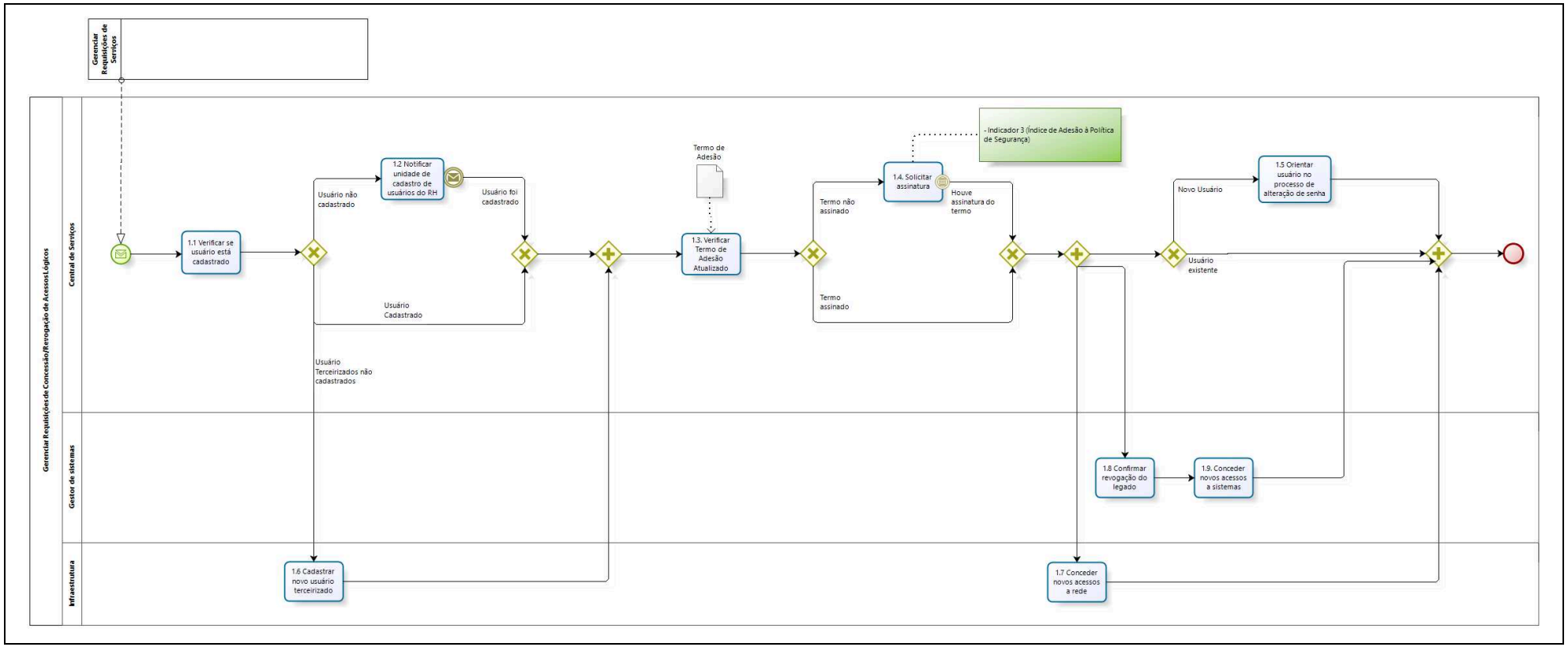
Equipe de monitoramento	• Verificar constantemente os sistemas de monitoramento em busca de eventos que comprometem ou podem comprometer a segurança física	Servidores designados
Central de Serviços	• Auxiliar os usuários nas tarefas de criação/alteração de senhas e certificados • Promover a assinatura do Termo de Adesão à Política de Segurança da Informação	Chefe do Setor de Gerenciamento da Central de Serviços
Gestor de Sistemas	• Conceder/revogar direitos de acessos a sistemas do qual seja gestor • Zelar pela aplicabilidade dos princípios de segregação de função e privilégio mínimo	Servidores do TRT24
Infraestrutura	• Cadastrar novo usuário terceirizado • Conceder novos acessos à rede	Servidores da Divisão de Infraestrutura de TIC

4.2. Fluxos do Processo

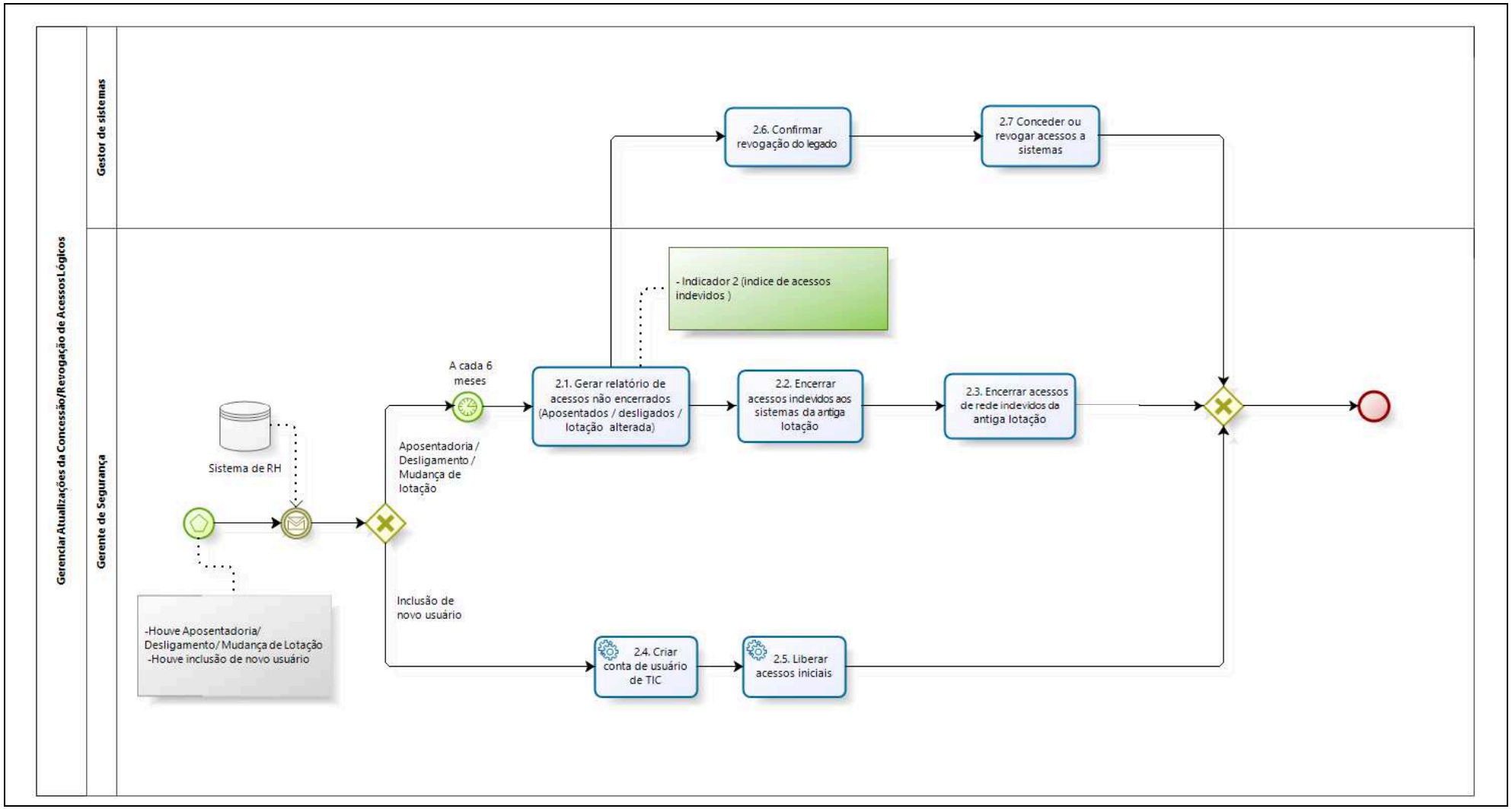
4.2.1. Fluxo Macro do Processo Gerenciar Controle de Acessos



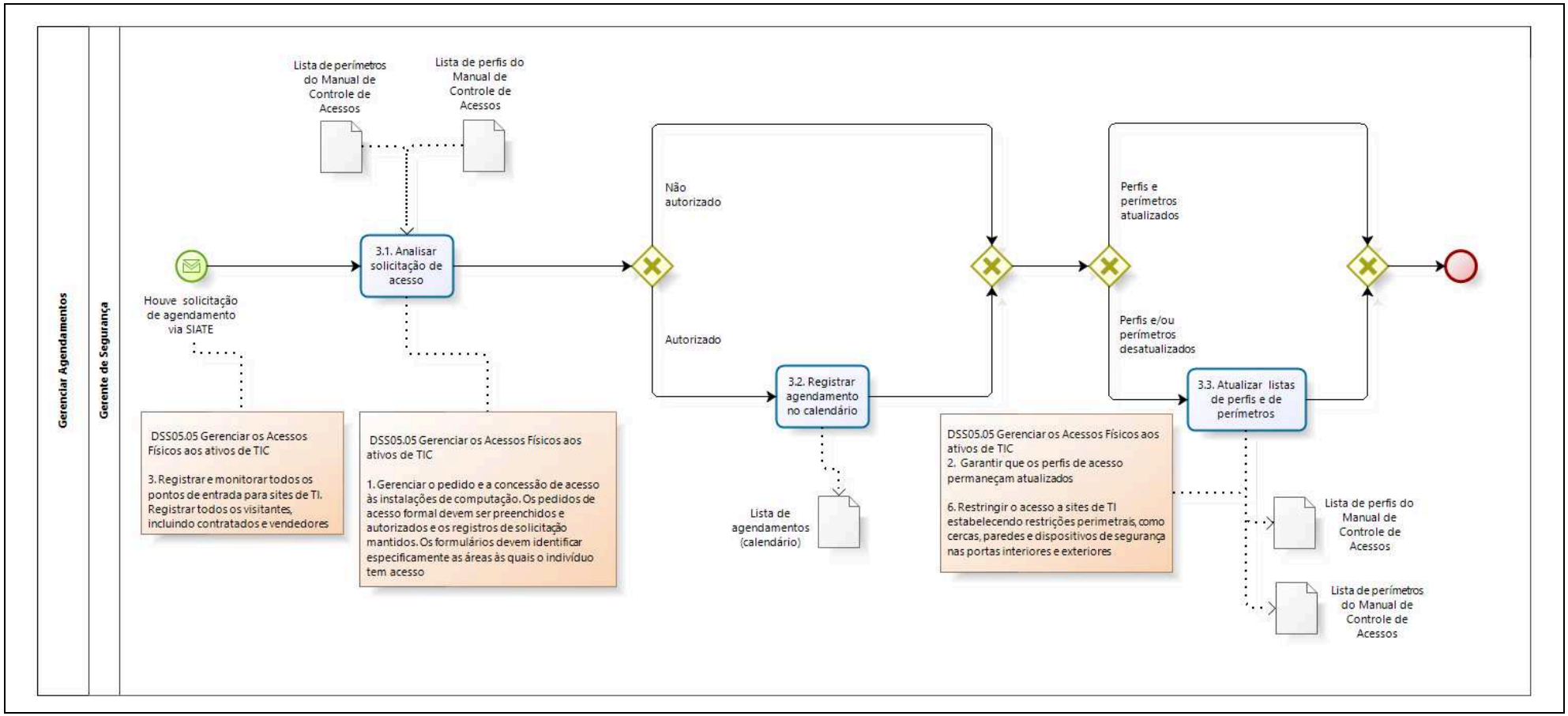
4.2.2. Fluxo Detalhado do Subprocesso Gerenciar Requisições de Concessão/Revogação de Acessos Lógicos



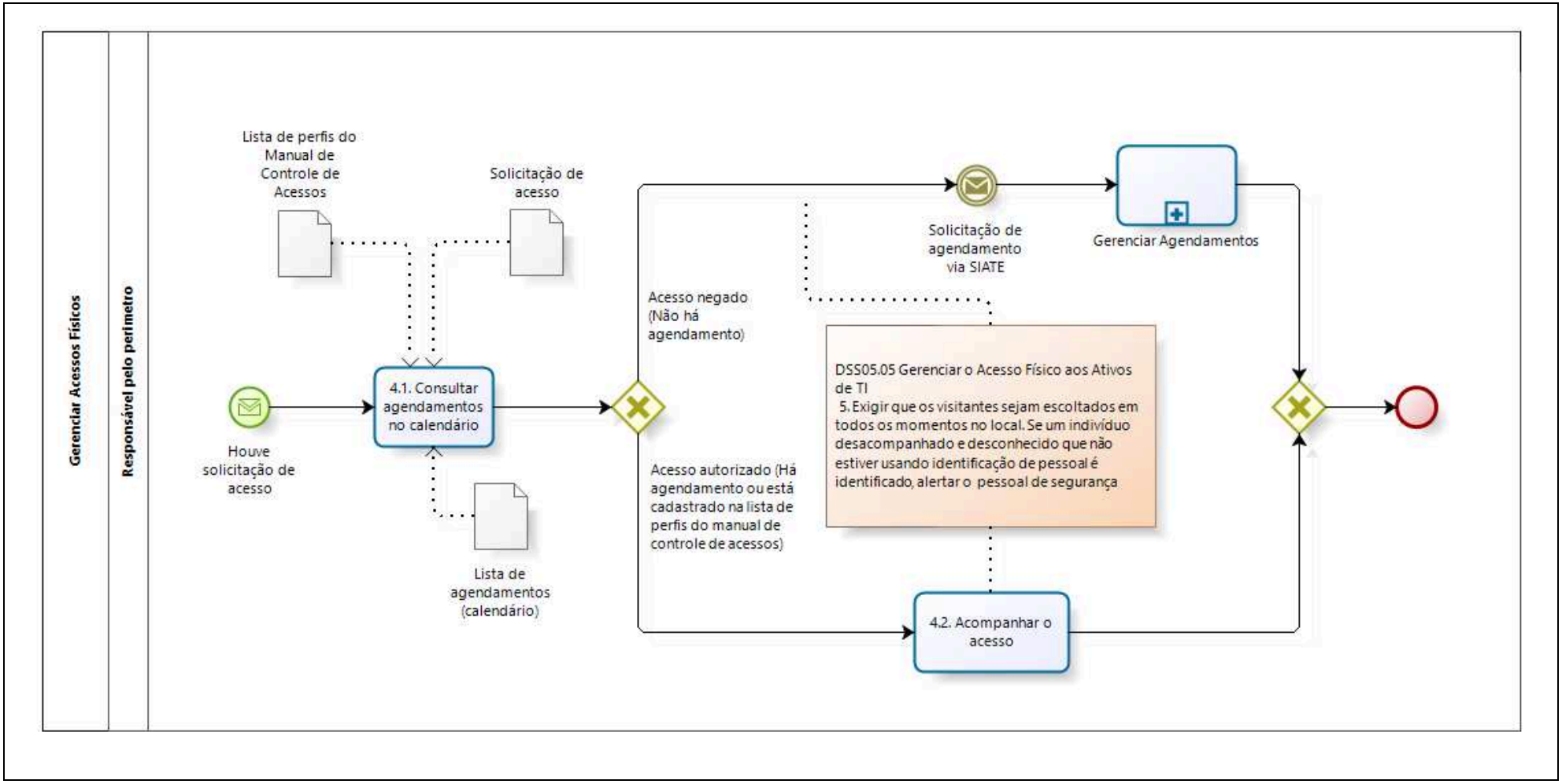
4.2.3. Fluxo Detalhado do Subprocesso Gerenciar Atualização de Concessão/Revogação de Acessos Lógicos



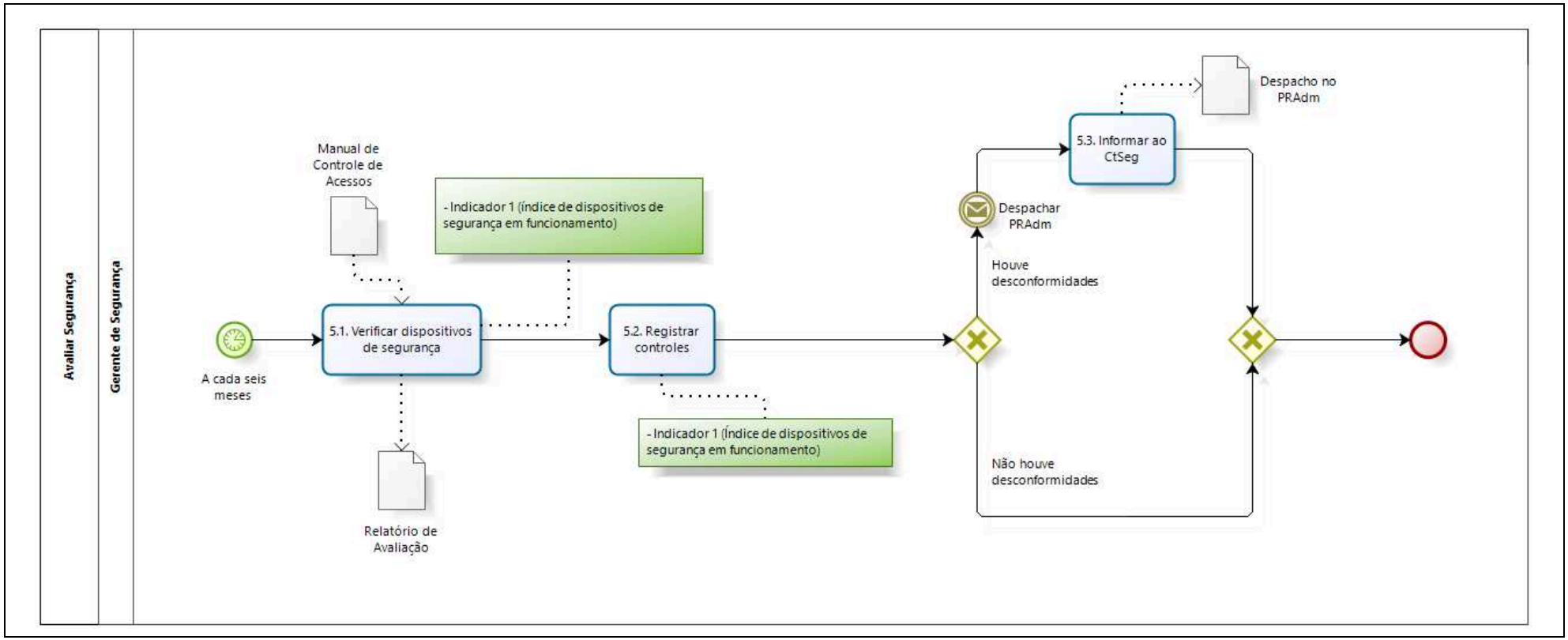
4.2.4. Fluxo Detalhado do Subprocesso Gerenciar Agendamentos



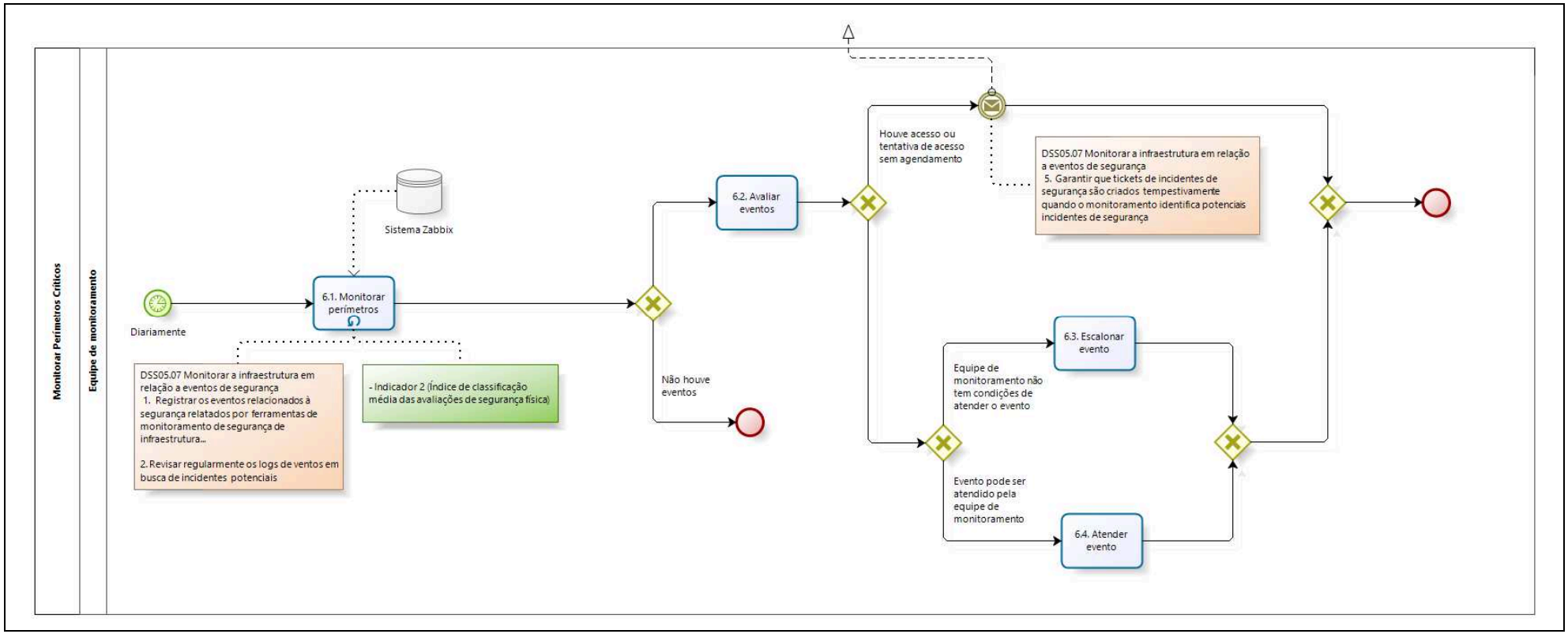
4.2.5. Fluxo Detalhado do Subprocesso Gerenciar Acessos Físicos



4.2.6. Fluxo Detalhado do Subprocesso Avaliar Segurança



4.2.7. Fluxo Detalhado do Subprocesso Monitorar Perímetros Críticos



4.3. Descrição do Processo

4.3.1. Descrição do Subprocesso Gerenciar Requisições de Concessão/Revogação de Acessos Lógicos

Id	Atividade	Responsável	Descrição
1.1	Verificar se usuário está cadastrado	Central de Serviços	**Entrada:** requisição de serviço
			Processamento: acessar o sistema SIGEP ou base de dados "Active Directory" e verificar se o usuário existe
			Saída: resultado da consulta ao cadastro do usuário
1.2	Notificar unidade de cadastro de usuários do RH	Central de Serviços	**Entrada:** resultado negativo na consulta pelo cadastro do usuário no sistema SIGEP ou base de dados "Active Directory"
			Processamento: notificar, por email ou telefone, a falta de cadastro das informações do usuário no sistema SIGEP para a unidade de cadastro de usuários do RH
			Saída: notificação da unidade de cadastro de usuários do RH
1.3	Verificar Termo de Adesão Atualizado	Central de Serviços	**Entrada:** Termos de Adesão cadastrados no PRADM 22420/2022
			Processamento: acessar o Sistema PROAD e verificar no PRADM 22420/2022 se o usuário assinou o Termo de Adesão à Política de Segurança da Informação
			Saída: consulta ao sistema PROAD
1.4	Solicitar assinatura	Central de Serviços	**Entrada:** resultado negativo da consulta ao sistema PROAD
			Processamento: • Entrar em contato com o gestor do usuário e solicitar a assinatura do Termo de Adesão pelo usuário (conforme modelo do ANEXO da Política de Controle de Acessos), bem como juntada no PRADM 22420/2022 • Explicar ao gestor e ao usuário que a assinatura do termo é condição indispensável para a concessão de direitos de acesso.
			Saída: Termo de Adesão assinado
1.5	Orientar usuário no processo de alteração de senha	Central de Serviços	**Entradas:** orientações da Central de Serviços
			Processamento: usar funcionalidade existente na Intranet ou Portal para substituir a senha inicial da conta de usuário de TIC por uma senha personalizada e que atenda às política de força e comprimento
			Saída: senha personalizada

1.6	Cadastrar novo usuário terceirizado	Infraestrutura	**Entrada:** Usuário terceirizado não cadastrado
			Processamento: cadastrar manualmente, no banco de dados "Active Directory", a conta do usuário terceirizado
			Saída: Usuário terceirizado cadastrado
1.7	Conceder novos acessos a rede	Infraestrutura	**Entrada:** requisição de acesso
			Processamento: • Conferir se os acessos requisitados são pertinentes ao usuário e sua respectiva lotação, seguindo se o princípio da segregação de funções e privilégios mínimos • Confirmar no Acordo de Nível Operacional se a concessão/revogação de acessos precisa de autorização superior • Em caso afirmativo para todos os itens acima, habilitar os direitos de acesso aos grupos e pastas da rede interna cabíveis ao requisitante
			Saída: acessos a rede do TRT24 habilitados
1.8	Confirmar revogação do legado	Gestor de sistemas	**Entrada:** Requisição de serviço ou e-mail de solicitação
			Processamento: • Buscar no sistema gerenciado eventuais direitos relativos a lotações anteriores a que o usuário não deveria mais ter acesso • Revogar todos os direitos indevidos eventualmente encontrados
			Saída: Direitos de acesso atualizados
1.9	Conceder novos acessos aos sistemas	Gestor de sistemas	**Entrada:** requisição de acesso ou e-mail de solicitação
			Processamento: • Conferir se o acesso requisitado está de acordo com os princípios de segregação de função e privilégio mínimo específicos ao sistema gerenciado • Conferir se o acesso requisitado é pertinente ao usuário • Confirmar se o acesso requisitado necessita de autorização superior • Em caso afirmativo para todos os itens acima, cadastrar no sistema gerenciado os acessos requisitados
			Saída: Direitos de acessos atualizados

4.3.2. Descrição do Subprocesso Gerenciar Atualizações de Concessão/Revogação de Acessos Lógicos

Id	Atividade	Responsável	Descrição
2.1	Gerar relatório de acessos não encerrados (Aposentados / desligados / lotação alterada)	Gerente de Segurança	**Entradas:** Lista de usuários desligados, aposentados ou com lotação alterada a mais de 2 meses e que ainda permaneçam com acessos legados indevidos
			Processamento: • Acessar cliente Oracle para acesso ao banco de dados do sistema SIGEP • Selecionar as views "sigep.vw_aposentados_3m" e "sigep.vw_desligados_20d" • Elaborar relatório a partir das seleções anteriores
			Saída: Relatório de acessos não encerrados
2.2	Encerrar acessos indevidos aos sistemas da antiga lotação	Gerente de Segurança	**Entradas:** Relatório de acessos não encerrados
			Processamento: Desativar os usuários do relatório no banco de dados do "Active Directory"
			Saídas: Desativação dos usuários no "Active Directory"
2.3	Encerrar acessos de rede indevidos da antiga lotação	Gerente de Segurança	**Entradas:** Relatório de acessos não encerrados
			Processamento: revogar os direitos de acesso aos grupos e pastas da rede interna e nuvem ou excluí-los do grupo relativo à antiga lotação em casos de mudança de lotação
			Saídas: revogação dos acessos aos grupos e pastas da rede interna e nuvem do TRT24
2.4	Criar conta de usuário de TIC	Gerente de Segurança **(Procedimento automático - trigger no Oracle)**	**Entrada:** cadastro de novo usuário de TIC no Sistema de Recursos Humanos - SIGEP
			Processamento: criar de uma identificação pessoal e intransferível, formada por login e senha, que permitirá ao novo usuário acessar os ativos de TIC.
			Saídas: nova conta de usuário criada
2.5	Liberar acessos iniciais	Gerente de Segurança **(Procedimento automático - trigger no Oracle)**	**Entrada:** nova conta de usuário
			Processamento: liberar acessos ao sistema AssineWeb e à Intranet/Portal
			Saídas: acesso liberado ao sistema AssineWeb e à Intranet/Portal
2.6	Revogar acessos a sistemas	Gestor de Sistemas	**Entradas:** Relatório de acessos não encerrados
			Processamento: Revogar todos os acessos existentes aos usuários constantes no relatório de acessos não encerrados
			Saída: acessos desativados

4.3.3. Descrição do Subprocesso Gerenciar Agendamentos

Id	Atividade	Responsável	Descrição
3.1	Analisar solicitação de acesso	Gerente de Segurança	**Entrada:** solicitação de agendamento via SIATE (formalizado pelo responsável pelo perímetro) e Manual de Controle de Acessos
			Processamento: validar os dados obrigatórios a constar no SIATE de solicitação (solicitante, data da solicitação, data do acesso, perímetros que serão acessados, justificativa para o acesso e identificação completa de quem irá acessar), analisar as informações da solicitação e das listas de perímetros e de perfis do Manual de Controle de Acessos para decidir se o solicitante poderá ou não entrar nos perímetros críticos
			Saída: autorização concedida ou negada
3.2	Registrar agendamento no calendário	Gerente de Segurança	**Entrada:** dados da solicitação de agendamento
			Processamento: registrar, em agenda compartilhada com responsáveis pelos perímetros, as informações pertinentes aos acessos solicitados
			Saída: lista de agendamento de acessos atualizada
3.3	Atualizar listas de perfis e de perímetros	Gerente de Segurança	**Entrada:** dados da solicitação de agendamento
			Processamento: avaliar os dados solicitação de agendamento e atualizar as informações de perfis e de perímetros críticos do Manual de Controle de Acessos
			Saída: lista de perfis e lista de perímetros atualizadas

4.3.4. Descrição do Subprocesso Gerenciar Acessos Físicos

Id	Atividade	Responsável	Descrição
4.1	Consultar agendamentos no calendário	Responsável pelo perímetro	**Entrada:** solicitação de acessos, lista de agendamentos (calendário), Manual de controle de acessos.
			Processamento: procurar na lista de agendamentos se a solicitação de acesso foi agendada ou se já está pré aprovada na Lista de perfis do manual de controle de acessos.
			Saída: acesso concedido ou negado
4.2	Acompanhar o acesso	Responsável pelo perímetro	**Entrada:** lista de agendamentos
			Processamento: • Verificar na lista de agendamento as informações pertinentes ao acesso • Acompanhar o solicitante pessoalmente durante o acesso ou designar algum servidor da SETIC para fazê-lo

4.3.5. Descrição do Subprocesso Avaliar Segurança

Id	Atividade	Responsável	Descrição
5.1	Verificar dispositivos de segurança	Gerente de Segurança	**Entrada:** lista de perímetros críticos e lista de dispositivos de segurança do Manual de Controle de Acessos
			Processamento: • Na capital o Avaliar em loco portas com cartão, portas com biometria e portas comuns o Avaliar remotamente através de software (Netbotz, CMC, Digifort) os dispositivos eletrônicos o Avaliar dispositivos de segurança lógica – firewall de borda, antivírus, ferramentas de monitoramento e auditoria • No interior o Avaliar com auxílio do responsável local (portas comuns e nobreak) o Avaliar através de software (netbotz) os dispositivos eletrônicos • Juntar o Relatório de Avaliação (conforme modelo do ANEXO VI) ao PRAdm do processo Gerenciar Controle de Acessos
			Saída: Relatório de Avaliação
5.2	Registrar controles	Gerente de Segurança	**Entrada:** PRADm (Relatório de Avaliação)
			Processamento: Registrar indicador 1, conforme planilhas do ANEXO I
			Saída: dados do indicador 1 registrado na planilha do ANEXO I
5.3	Informar ao CTSeg	Gerente de Segurança	**Entrada:** PRAdm
			Processamento: Despachar no PRAdm informando ao Comitê de Segurança as eventuais ocorrências apuradas na verificação
			Saída: PRAdm encaminhado ao CtSeg

4.3.6. Descrição do Subprocesso Monitorar Perímetros Críticos

Id	Atividade	Responsável	Descrição
6.1	Monitorar perímetros	Equipe de monitoramento	**Entrada:** dados do sistema Zabbix, senhasegura, loqed e varonis
			Processamento: Observar continuamente as informações apresentadas pelos sistemas Zabbix, loqed e varonis nas TVs de monitoramento de segurança e registrar os eventos pertinentes. Utilizar o sistema senhasegura caso seja necessário monitorar acessos em execução ou já realizados.
6.2	Avaliar eventos	Equipe de monitoramento	**Entrada:** alertas do sistema Zabbix, senhasegura, loqed e varonis
			Processamento: Analisar e avaliar as providências pertinentes aos eventuais alertas emitidos pelo sistema , senhasegura, loqed e varonis
			Saída: diagnóstico da situação decorrente do alerta
6.3	Escalonar evento	Equipe de monitoramento	**Entrada:** Alerta do sistema Zabbix, senhasegura, loqed e varonis e diagnóstico do alerta
			Processamento: Solicitar apoio da(s) área(s) relacionadas ao alerta
			Saída: Evento encaminhado para solução por outra área da SETIC
6.4	Atender evento	Equipe de monitoramento	**Entrada:** Alerta do sistema Zabbix, senhasegura, loqed e varonis e diagnóstico do alerta
			Processamento: Atuar no atendimento do evento, conforme procedimentos pertinentes
			Saída: Evento atendido e solucionado

5. Tabela RACI

5.1. Subprocesso Gerenciar Requisições de Concessão/Revogação de Acessos Lógicos

	Atividade	Central de Serviços	Infraestrutura	Gestor de sistemas	Usuários de TI
1.1	Verificar se usuário está cadastrado	**R**	**I**		
1.2	Notificar unidade de cadastro de usuários do RH	**R**			
1.3	Verificar Termo de Adesão atualizado	**R**			
1.4	Solicitar assinatura	**R**			**C**
1.5	Orientar usuário no processo de alteração de senha	**R**			**I**
1.6	Cadastrar novo usuário terceirizado	**I**	**R**		**I**
1.7	Conceder novos acessos a rede	**I**	**R**		**I**
1.8	Confirmar revogação do legado			**R**	
1.9	Conceder novos acessos a sistemas			**R**	**I**

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

5.2. Subprocesso Gerenciar Atualizações de Concessão/Revogação de Acessos Lógicos

	Atividade	Central de Serviços	Gerente de Segurança	Gestor de Sistemas
2.1	Gerar relatório de acessos não encerrados (Aposentados / desligados / lotação alterada)		**R**	
2.2	Encerrar acessos indevidos aos sistemas da antiga lotação		**R**	
2.2	Encerrar acessos de rede indevidos da antiga lotação		**R**	
2.3	Criar conta de usuário de TIC		**R**	
2.5	Liberar acessos iniciais		**R**	
2.6	Revogar acessos a sistemas			**R**

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

5.3. Subprocesso Gerenciar Agendamentos

	Atividade	Gerente de Segurança	Responsável pelo perímetro
3.1	Analisar solicitação de acesso	**R**	**C**

	Atividade	Gerente de Segurança	Responsável pelo perímetro
3.2	Registrar agendamento no calendário	**R**	**I**
3.3	Atualizar listas de perfis e de perímetros	**R**	**C**

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

5.4. Subprocesso Gerenciar Acessos Físicos

	Atividade	Gerente de Segurança	Responsável pelo perímetro
4.1	Consultar agendamentos no calendário		**R**
4.2	Acompanhar o acesso	**I**	**R**

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

5.5. Subprocesso Avaliar Segurança

	Atividade	Gerente de Segurança	Responsável pelo perímetro
5.1	Verificar dispositivos de segurança	**R**	**I**
5.2	Registrar controles	**R**	
5.3	Informar ao CTSeg	**R**	

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

5.6. Subprocesso Monitorar Perímetros Críticos

	Atividade	Gerente de Segurança	Equipe de Monitoramento
6.1	Monitorar perímetros	**I**	**R**
6.2	Avaliar eventos	**C**	**R**
6.3	Escalonar evento	**I**	**R**
6.4	Atender evento	**I**	**R**

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

6. Controles do Processo

O controle do processo é realizado por meio de indicadores obtidos através da coleta de dados relacionados ao processo, sendo que, quando os resultados esperados não forem alcançados, devem ser estabelecidas ações para tratamento dos desvios encontrados.

6.1. Controles COBIT 5.0

Id	Objetivo do processo (*process goal*)	Indicador
1	Medidas físicas foram implementadas para proteger informações de acessos não autorizados, danos e interferências ao serem processados, armazenados ou transmitidos	Índice de dispositivos de segurança em funcionamento

6.2. Controles Elaborados

Id	Objetivo	Indicador
2	Medir a eficiência da comunicação e dos mecanismos e procedimentos externos de revogação de acessos indevidos	Índice de acessos indevidos
3	Medir a taxa de assinatura do Termo de Adesão	Índice de adesão à Política de Segurança da Informação

1) Índice de dispositivos de segurança em funcionamento

Origem	• **DSS05 (Gerenciar Serviços de Segurança)**
	  ○ **PAM outcome**: DSS05-04
	  ○ **Supports**: PAM base practices DSS05-BP5
	  ▪ **Enabling process:** Key management practices DSS05.05

Meta	50%
Periodicidade	Semestral
Forma de cálculo	Total de dispositivos em funcionamento / Total de dispositivos
Fonte	• Planilha do ANEXO I ○ **Total de dispositivos em funcionamento**: ver o valor da coluna “Quantidade de dispositivos em funcionamento”

	○ **Total de dispositivos**: ver o valor da coluna "Quantidade de dispositivos"

2) Índice de Acessos Indevidos

Origem	Controle elaborado pela DPDSEG
Periodicidade	Semestral
Meta	Menor que 15%
Forma de cálculo	(Total de usuários que deveriam estar com acessos revogados / Total de usuário de TIC) x 100
Fonte	• Planilha do ANEXO III ○ **Total de usuários que deveriam estar com acessos revogados:** ver o valor da coluna "Quantidade de usuários que deveriam estar com acessos revogados" correspondente a última apuração ○ **Total de usuários de TIC**: ver o valor da coluna "Quantidade de usuários de TIC" correspondente a última apuração

3) Índice de Adesão à política de Segurança da Informação

Origem	Controle elaborado pela DPDSEG
Periodicidade	Semestral
Meta	90%
Forma de cálculo	(Total de termos assinados / Total de usuário de TIC) x 100
Fonte	• Planilha do ANEXO III ○ **Total de termos assinados**: ver o valor da coluna "Quantidade de Termos de Adesão assinados" correspondente a última apuração ○ **Total de usuários de TIC**: ver o valor da coluna "Quantidade de usuários de TIC" correspondente a última apuração

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 Controle de Acessos**.

1. ANEXO I – Indicador 1 (Índice de dispositivos de segurança em funcionamento)

Data da apuração	Quantidade de dispositivos em funcionamento	Quantidade de dispositivos

Onde

- Para cada apuração:
  - **Data da apuração**: data em que os dados estão sendo apurados
  - **Quantidade de dispositivos em funcionamento**: informar a quantidade de dispositivos testados que estão operacionais (considerar a lista de perímetros e dispositivos prevista no Manual de Controle de Acessos). Dispositivos não testados devem ser considerados como em "**Não Funcionamento"**.
  - **Quantidade de dispositivos**: informar a quantidade de dispositivos de segurança da lista de perímetros do Manual de Controle de Acessos.

2. ANEXO II – Indicador 2 (Índice de Acessos Indevidos)

Data da apuração	Quantidade de usuários que deveriam estar com acessos revogados	Quantidade de usuários de TIC

Onde

- Para cada apuração:
  - **Data da apuração**: data em que os dados estão sendo apurados
  - **Quantidade de usuários que deveriam estar com acessos revogados:** informar a quantidade de usuários que deveriam estar com os acessos revogados mas não estão com base nas “views” do SIGEP.
  - **Quantidade de usuários de TIC**: informar a quantidade de usuários de TIC no momento da apuração, com base no relatório usuários do SIGEP (somente situações funcionais pertinentes).

3. ANEXO III – Indicador 3 (Índice de adesão à Política de Segurança da Informação)

Data da apuração	Quantidade de Termos de Adesão assinados	Quantidade de usuários de TIC

Onde

- Para cada apuração:
  - **Data da apuração**: data em que os dados estão sendo apurados
  - **Quantidade de Termos de Adesão assinados**: informar a quantidade de termos de Adesão assinados até o momento da apuração
  - **Quantidade de usuários de TIC**: informar a quantidade de usuários de TIC no momento da apuração, com base no relatório de usuários do SIGEP (somente situações funcionais pertinentes)

11. ANEXO IV – Modelo de formulário de Solicitação de Agendamento de Acesso Físico

SETIC – Secretaria da Tecnologia de Informação e Comunicações

Formulário de Solicitação de Agendamento de Acesso Físico

Identificação

1.1 Nº da solicitação		*Data da solicitação*	____/____/____
1.3 Solicitante			
1.4 Data do acesso	____/____/____		
1.5 Perímetros que serão acessados			
1.6 Justificativa para o acesso			
1.7 Quem irá acessar			

Referência:

- **Nº da solicitação**: número do SIATE para fins de controle
- **Data da solicitação**: data em que o pedido foi apresentado ao Gerente de Segurança
- **Nome do solicitante**: nome de quem está solicitando o acesso
- **Data do acesso**: data em que o solicitante pretende entrar no perímetro
- **Perímetros que serão acessados**: áreas as quais o solicitante deseja entrar
- **Justificativa para o acesso**: qual é o problema ou a razão que motivam o solicitante a entrar no perímetro crítico?
- **Quem irá acessar**: nome de quem irá acessar o perímetro

OBS: Acessos físicos serão requisitados via SIATE e não mais neste modelo, conforme concordância na reunião de atualização do processo;

12. ANEXO V – Modelo de Relatório de Avaliação

Perímetro Crítico	*Lista de Dispositivos*	*Avaliação*	*Portas*	*Avaliação*
Sala cofre no prédio sede	Sensor de temperatura e umidade			
	Dispositivo "Stratos" para detecção antecipada de incêndios			
	Sensor de temperatura e umidade da Sala POP			
	Sensor de temperatura e umidade da Sala UPS			
	Dispositivo de acesso biométrico por digital			
	Sensor de abertura da porta			
	Câmeras de vídeo com histórico de 30 dias			
	UPS – "Uninterrupted Power Suply device"			
	Gerador de energia			
Sala dos módulos de segurança no prédio sede (1º andar)	Sensor de umidade			
	Sensor de temperatura			
	Sensor de fluxo de ar			
	Câmera de segurança via imagem com histórico de 24 horas			
	Porta com acesso controlado via cartão magnético			
Salas técnicas das unidades do interior	Sensor de umidade			
	Sensor de temperatura			
	Sensor de fluxo de ar			
	Câmera de segurança via imagem com histórico de 24 horas			
	Porta com acesso controlado via cartão magnético			

Sala técnica no prédio do Foro Trabalhista da capital (site backup)	Sensor de umidade			
	Sensor de temperatura			
	Sensor de fluxo de ar			
	Câmera de segurança via imagem com histórico de 24 horas			
	Porta com acesso controlado via cartão magnético			
	Nobreak			
Salas técnicas auxiliares	Rack com fechadura e chave			
	NoBreak			
Dispositivos de segurança lógica	Firewall/IPS de borda			
	Antivírus			
	Loqed			
	Varonis			
	Senha Segura			