Poder Judiciário
Justiça do Trabalho
Tribunal Regional do Trabalho da 13ª Região

ATO TRT SGP N.º 139, DE 15 DE DEZEMBRO DE 2020

Institui o Processo de Gerenciamento de Acesso e uso de Recursos de TIC.

O DESEMBARGADOR PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA DÉCIMA TERCEIRA REGIÃO, no uso de suas atribuições legais e regimentais,

considerando as diretrizes da Política de Segurança da Informação e Comunicação da instituição;

considerando a necessidade de manter a continuidade dos serviços essenciais que a instituição presta à sociedade;

considerando a legislação federal, assim como resoluções, normas, recomendações e boas práticas publicadas pelo CNJ, CSJT, TCU e ABNT relacionadas à Segurança da Informação;

considerando a Exposição de Motivos constante do Protocolo n.º 000-09768/2020,

R E S O L V E:

Art. 1º Este Ato estabelece o Processo de Gerenciamento de Acesso e Uso de Recursos de TIC no âmbito do Tribunal Regional do Trabalho da 13ª Região.

Art. 2º A descrição, os papéis e as responsabilidades do processo, referido no art.1º, encontram-se estabelecidos no Anexo I deste Ato.

Art. 3º O presente Ato entra em vigor na data de sua publicação.

Dê-se ciência.
Publique-se no DA_e.

(assinado eletronicamente)
WOLNEY DE MACEDO CORDEIRO
Desembargador Presidente

Tribunal Regional do Trabalho
13ª Região | Paraíba

Tribunal Regional do Trabalho
13ª Região | Paraíba

MANUAL DO PROCESSO DE GERENCIAMENTO DE ACESSOS E USO DE RECURSOS DE TIC

Seção de Segurança da Informação

João Pessoa – 2020
Versão 1.0

Tribunal Regional do Trabalho da 13ª Região

Desembargador Presidente

Wolney de Macedo Cordeiro

Comitê Gestor de Segurança da Informação

Lindinaldo Silva Marinho (Presidente)

Antônio Fragoso Cavalcante Neto

Francisco Hirllen de Oliveira Mendonça

Isêlma Maria de Souza Rodrigues

Rodrigo Cartaxo Marques Duarte

Rodrigo Mafra

Seção de Segurança da Informação

Rodrigo Mafra (Chefe)

Manuel Rodrigues Vieira da Silva

SUMÁRIO

Sumário

1. Objetivo

Definir o Processo de Gerenciamento de Acessos e Uso de Recursos de TIC.

2. Propósito do processo

Este processo tem como propósito nortear a concessão, revogação e alteração de permissões de acesso aos usuários de recursos de TIC no âmbito do Tribunal Regional do Trabalho – 13ª Região, em conformidade com as normas de segurança da informação da instituição.

3. Escopo

O escopo do processo compreende todos os serviços de TIC oferecidos pela SETIC – Secretaria de Tecnologia da Informação e Comunicação do TRT da 13ª Região.

4. Definições e abreviações

Para efeitos deste manual, aplicam-se as definições da Política de Segurança da Informação e Comunicações (POSIC), além das seguintes:

- **Credencial:** conjunto de atributos que identifica univocamente um usuário, previamente cadastrado, para concessão de acesso aos recursos de TIC. Ex.: login e senha, endereço de e-mail e senha, certificado digital e senha, características biométricas, etc;
- **Acesso:** permissão de uso dos recursos de TIC, concedida ao usuário mediante apresentação de uma credencial válida;
- **Nome do usuário (login):** identificador único de cada usuário para acesso aos recursos de TIC**;**
- **Senha:** conjunto de caracteres, de uso e conhecimento exclusivo do usuário, que permite autenticá-lo e, assim, conceder o acesso aos recursos de TIC;
- **Permissões:** conjunto de direitos que um usuário possui para acessar os recursos de TIC e as informações disponíveis nos mesmos. Devem ser as mínimas necessárias para que o usuário possa utilizar os recursos adequadamente;
- **Autenticação:** processo pelo qual o usuário apresenta uma credencial para obter acesso aos recursos de TIC;
- **Base de Dados de Credenciais**: banco de dados, preferencialmente centralizado, onde são armazenadas todos as informações dos usuários necessárias para acesso aos serviços/sistemas de TIC, tais como credenciais, permissões, etc;

- **Base de Dados de Pessoas**: banco de dados, preferencialmente centralizado, onde são armazenadas todas as informações de pessoas vinculadas à instituição: magistrados, servidores, estagiários, terceirizados, etc.
- ***Logs* de Acesso**: arquivos com os registros de acessos dos usuários aos sistemas/serviços de TIC da instituição.

5. Benefícios esperados

A implementação do Processo de Gerenciamento de Acessos e Uso de Recursos de TIC no TRT da 13ª Região promoverá os seguintes benefícios:

- Aderência à Política de Segurança da Informação e Comunicações (POSIC) da instituição, promovendo a confidencialidade, disponibilidade e integridade das informações.

6. Interfaces com demais processos

- **Processo de Gestão de Riscos de Segurança da Informação**: a concessão de permissões mínimas e adequadas para os usuários acessarem os recursos de TIC contribui para a diminuição dos riscos de Segurança da Informação.

7. Entradas e saídas

As principais entradas e saídas do Processo de Gerenciamento de Acessos e Uso de Recursos de TIC são:

7.1 Entradas

- Ato ou Portaria que implique na concessão, alteração ou revogação de permissões de acesso;
- Chamados;
- *Logs* de Acesso;
- Base de Dados de Pessoas.

7.2 Saídas

- Base de Dados de Credenciais atualizada, contendo os usuários com as permissões adequadas de acesso aos recursos de TIC da instituição;
- Relatório de Revisão de Credenciais.

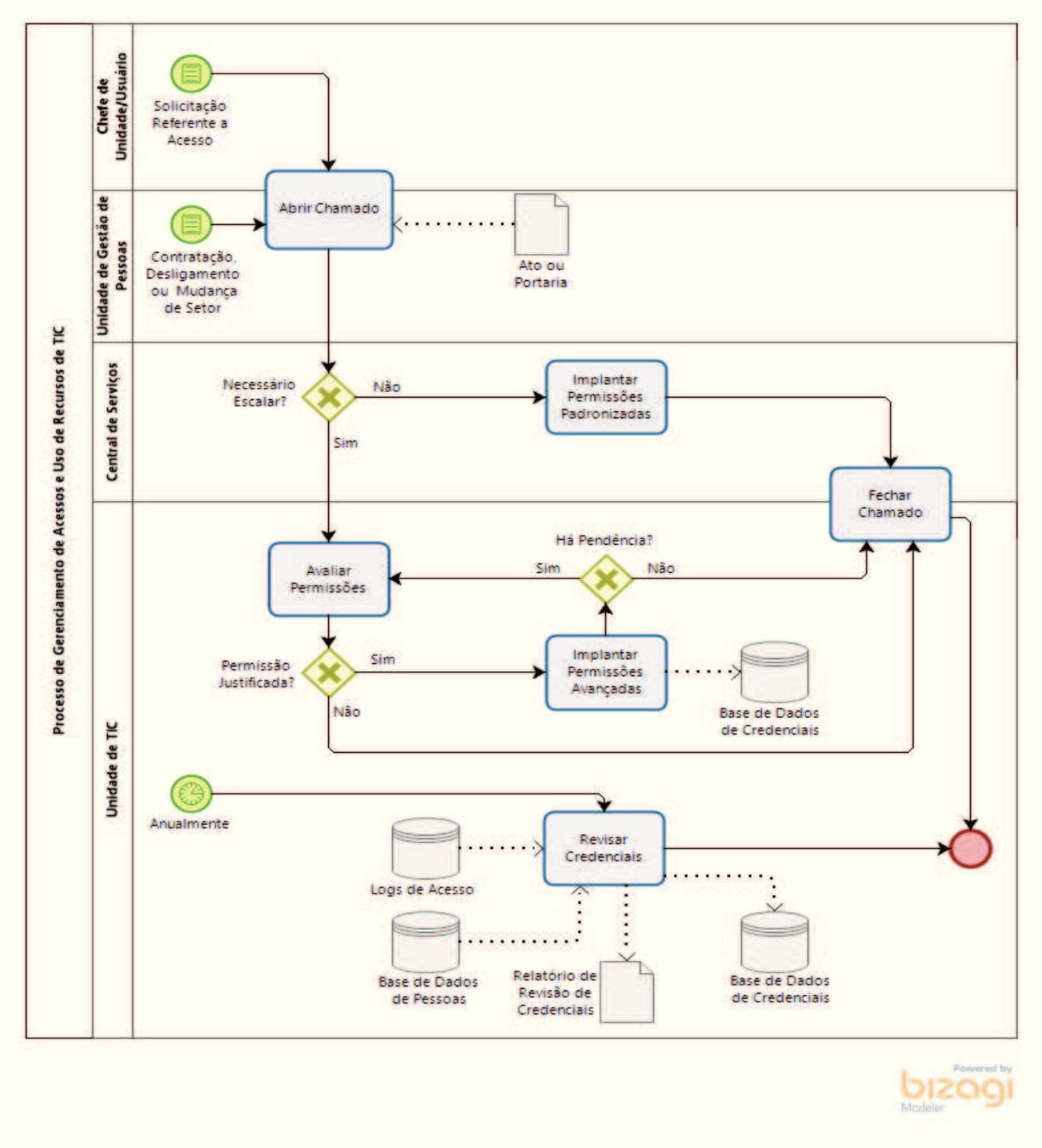
8. Papéis e responsabilidades

Abaixo estão definidos os papéis, seus executores e suas responsabilidades:

PAPEL	DESCRIÇÃO	RESPONSABILIDADES
Chefe de Unidade/ Usuário	Chefe de Unidade da instituição ou Usuário conforme POSIC.	Solicitar concessão, revogação ou alteração de credenciais e permissões de acesso aos recursos de TIC, de acordo com a necessidade da unidade ou do usuário e com fundamentação em ato, norma ou legislação pertinente.
Unidade de Gestão de Pessoas	Unidade responsável pela gestão de pessoas na instituição.	Solicitar concessão, revogação ou alteração de credenciais e permissões de acesso aos recursos de TIC, de acordo com eventos de Gestão de Pessoas fundamentados por atos de autoridade competente.
Central de Serviços	Equipe da área de TIC responsável pelo atendimento de primeiro nível e pela triagem dos chamados.	Encaminhar chamado para Unidades de TIC quando necessário.
		Implantar permissões padronizadas nos ativos de TIC.
		Encerrar chamado.
Unidade de TIC	Compreende as unidades técnicas da área de TIC, responsáveis por administrar os serviços e recursos de TIC da instituição.	Implantar permissões avançadas nos ativos de TIC sob sua responsabilidade.
		Revisar Base de Dados de Credenciais dos ativos sob sua responsabilidade.
		Encerrar chamado.
Unidade de Segurança da Informação (SI)	Unidade responsável pelo macroprocesso de Segurança da Informação e pelo Processo de Gerenciamento de Acessos e Uso de Recursos de TIC.	Manter atualizada a documentação do Processo de Gerenciamento de Acessos e Uso de Recursos de TIC.

9. O Processo de Gerenciamento de Acessos e Uso de Recursos de TIC

O Processo de Gerenciamento de Acessos e Uso de Recursos de TIC é mostrado no diagrama a seguir. Logo abaixo são descritas as atividades do processo.



Abrir Chamado		
Descrição	Abrir chamado visando a concessão, revogação ou alteração de permissões de acesso aos recursos de TIC da instituição.	
Considerações importantes	N/A	
Papéis	Chefe de Unidade, Usuário, Unidade de Gestão de Pessoas.	
Entradas	Ato ou Portaria que implique na concessão, revogação ou alteração de permissões de acesso aos recursos de TIC da instituição.	
Saídas	Chamado com solicitação de concessão, revogação ou alteração de permissões de acesso aos recursos de TIC da instituição.	
Atividades	**Abrir chamado**	Abrir chamado pelos canais apropriados.
Modelos	N/A	

Avaliar Permissões		
Descrição	Avaliar se a solicitação de concessão, revogação ou alteração de permissões de acesso aos recursos de TIC da instituição pode ser atendida.	
Considerações importantes	N/A	
Papéis	Unidades de TIC.	
Entradas	Chamado com solicitação de concessão, revogação ou alteração de permissões de acesso aos recursos de TIC da instituição.	
Saídas	Chamado com solicitação de concessão, revogação ou alteração de permissões de acesso aos recursos de TIC da instituição atualizado.	
Atividades	**Avaliar Permissões**	Verificar se a solicitação de concessão, revogação ou alteração de permissões de acesso aos recursos de TIC pode ser atendida. A solicitação só poderá ser atendida quando justificada/fundamentada por ato, norma ou legislação. Pode ser necessária confirmação com o solicitante ou superior do mesmo.
	Atualizar Chamado	Registrar no chamado se o mesmo poderá ser atendido ou não e a justificativa para isso.
Modelos	N/A	

Implantar Permissões Padronizadas		
Descrição	Implantar Permissões Padronizadas nos serviços de TIC da instituição.	
Considerações importantes	N/A	
Papéis	Central de Serviços.	
Entradas	Chamado com solicitação de concessão, revogação ou alteração de permissões de acesso aos recursos de TIC da instituição.	
Saídas	Chamado com solicitação de concessão, revogação ou alteração de permissões de acesso aos recursos de TIC da instituição atualizado.	
Atividades	**Avaliar permissões**	Avaliar se a solicitação pode ser atendida de acordo com os procedimentos padronizados.
	Implantar Permissões	Implantar, quando possível, as permissões solicitadas nos serviços de TIC da instituição de acordo com os procedimentos padronizados.
	Atualizar chamado	Registrar no chamado se a solicitação foi atendida ou não e a justificativa para isso.
Modelos	N/A	

Implantar Permissões Avançadas		
Descrição	Implantar Permissões Avançadas nos ativos/serviços de TIC da instituição.	
Considerações importantes	N/A	
Papéis	Unidade de TIC	
Entradas	Chamado com solicitação de concessão, revogação ou alteração de permissões de acesso aos recursos de TIC da instituição.	
Saídas	Chamado com solicitação de concessão, revogação ou alteração de permissões de acesso aos recursos de TIC da instituição atualizado. Base de Dados de Credenciais atualizada.	
Atividades	**Criar Usuário**	Criar usuário, caso necessário, na Base de Dados de Credenciais.
	Desativar Usuário	Desativar usuário, caso necessário, na Base de Dados de Credenciais.
	Implantar Permissões Avançadas	Conceder, Revogar e/ou Alterar as permissões de acesso aos recursos de TIC solicitados, atualizando Base de Dados de Credenciais.
	Atualizar chamado	Atualizar o chamado com todas as informações pertinentes. Encaminhar o mesmo para outra Unidade de TIC se houver pendência. Ir para Fechar Chamado caso contrário.
Modelos	N/A	

Fechar Chamado		
Descrição	Fechar Chamado após implantação das permissões ou quando não for possível implantá-las.	
Considerações importantes	N/A	
Papéis	Central de Serviços, Unidade de TIC.	
Entradas	Chamado com solicitação de concessão, revogação ou alteração de permissões de acesso aos recursos de TIC da instituição.	
Saídas	Chamado com solicitação de concessão, revogação ou alteração de permissões de acesso aos recursos de TIC da instituição fechado.	
	Fechar chamado	Fechar o chamado, informando se as permissões foram concedias ou não e a justificativa para isso.
Modelos	N/A	

Revisar Credenciais		
Descrição	Revisar anualmente a Base de Dados de Credenciais.	
Considerações importantes	O Relatório de Revisão de Credenciais deve conter para cada Base de Dados de Credenciais revisada: - Número total de usuários ativos antes da revisão; - Número de usuários com permissões corrigidas.	
Papéis	Unidade de TIC.	
Entradas	*Logs* de Acesso, Base de Dados de Credenciais e Base de Dados de Pessoas.	
Saídas	Base de Dados de Credenciais atualizada. Relatório de Revisão de Credenciais.	
Atividades	**Avaliar *logs* de acesso**	Avaliar os arquivos de *logs* de acesso para identificar os usuários com acessos suspeitos.
	Verificar inconsistências	Verificar inconsistências entre a Base de Dados de Pessoas e Base de Dados de Credenciais e determinar permissões inadequadas.
	Corrigir Permissões	Corrigir, na Base de Dados de Credenciais, as permissões que estão configuradas inadequadamente detectadas nas duas atividades acima.
	Fazer Relatório de Revisão de Credenciais	Fazer e arquivar relatório de Revisão de Credenciais.
Modelos	N/A	

10. Indicadores de desempenho

10.1 Eficácia do Processo de Gerenciamento de Acessos e Uso de Recursos de TIC

Indicador 1	
Objetivo	Avaliar a eficácia do Processo de Gerenciamento de Acessos e Uso de Recursos de TIC.
Indicador	Percentual de Permissões de Acesso Revisadas = Número total de usuários com permissões corrigidas em todas as Bases de Dados de Credenciais / Número total de usuários ativos em todas as Bases de Dados de Credenciais antes da revisão * 100.
Responsável pela medição	Unidade de Segurança da Informação (SI).
Período de Medição	Anual.

10.2 Eficiência do Processo de Gerenciamento de Acessos e Uso de Recursos de TIC

Indicador 1	
Objetivo	Avaliar a eficiência do Processo de Gerenciamento de Acessos e Uso de Recursos de TIC.
Indicador	Tempo médio dos chamados com solicitação de concessão, revogação ou alteração de permissões de acesso aos recursos de TIC da instituição.
Responsável pela medição	Unidade de Segurança da Informação (SI).
Período de Medição	Anual.