Procedimentos e Critérios para Concessão de Acesso aos Módulos do SIGEP-JT

Abril de 2024

Versão 1.1

Sumário

Apuração de Gratificação por Exercício de Cumulativo de Jurisdição (GECJ)

Procedimento e Critérios para Concessão de Acesso ao Módulo Apuração de Gratificação por Exercício de Cumulativo de Jurisdição (GECJ)

Procedimento para Concessão de Acesso

O GECJ utiliza o keycloak para autenticação, e controle de autenticação por perfis dinâmicos configurados nos próprios sistemas.

Atualmente o sistema só permite o acesso por usuário deve ser um servidor/magistrado cadastrado no SIGEP (srh2.servidor) e que possa ser autenticado pelo keycloak.

Para configurar o perfil, acessar o menu Gerencial → Gerenciar Permissões de Acesso.

Incluir novo perfil com nome “Auditor” e selecionar as seguintes permissões na aba Permissões:

- Permissão para acessar a tela de consulta de magistrados.
- Permissão para imprimir o cálculo mensal na tela de histórico.

Em seguida, na aba Vínculos, incluir em “Usuários Vinculados” o usuário que será utilizado pelo auditor.

Uma vez concedido o perfil, basta fazer novo login no módulo para que as atualizações de perfis concedidos sejam processadas.

Critérios para Acesso do Perfil Auditor

O perfil Auditor pode ser configurado dinamicamente no GECJ. Podem ser vinculadas a este perfil quaisquer funcionalidades que julgarem necessárias para atuação do auditor.

Ártemis - Indicação e Remoção de Servidores (ART)

Procedimento e Critérios para Concessão de Acesso ao Módulo Ártemis - ART

Procedimento para Concessão de Acesso

Para a concessão de acesso a perfis no módulo Ártemis, o usuário precisa estar visível na mview IRH.MV_RH_PORTAL. A implementação desta view é feita na instalação do módulo nacional de Controle de Acesso em cada Regional, conforme as instruções existentes da Wiki San-Doc.

Após o usuário estar criado, deve ser formalizada uma solicitação ao Gestor de Controle de Acesso do módulo/submódulo para que este, a partir do módulo de Controle de Acesso, faça a atribuição do perfil.

O módulo de Controle de Acesso está disponível no Portal SISAD e permite a atribuição de perfis por quatro critérios:

- Por usuário: perfil concedido individualmente a um usuário específico
- Por lotação: perfil concedido a todos os usuários lotados na unidade organizacional informada
- Por cargo: perfil concedido a todos os usuários que ocupem o cargo informado
- Por categoria: perfil concedido a todos os usuários que atendam os critérios da categoria[1] informada.

Uma vez concedido o perfil via módulo de Controle de Acesso, basta fazer novo login no módulo para que as atualizações de perfis concedidos sejam processadas e o usuário possa utilizá-los.

Critérios para Acesso do Perfil Auditor

O perfil Auditor ainda não está implementado no módulo Ártemis, mas entende-se que, de acordo com a explicação dada pela Auditora da CCAUD/CSJT em reunião do gtControleAcessoSIGEP, este perfil deve dar acesso de consulta a **todas** as telas do sistema.

Os perfis atuais do sistema e a previsão dos direitos a serem concedidos ao perfil Auditor podem ser consultados na planilha Mapa de Perfis de Acesso

[1] O módulo de Controle de Acesso permite a criação de categorias, pelos Regionais, que atendam às suas necessidades.

Atualização Cadastral de Inativos e Pensionistas (ACIP)

Procedimento e Critérios para Concessão de Acesso ao Módulo Atualização Cadastral de Inativos e Pensionistas - ACIP

Procedimento para Concessão de Acesso

Para a concessão de acesso a perfis no módulo Atualização Cadastral de Inativos e Pensionistas, o usuário precisa estar visível na mview IRH.MV_RH_PORTAL. A implementação desta view é feita na instalação do módulo nacional de Controle de Acesso em cada Regional, conforme as instruções existentes da Wiki San-Doc.

Após o usuário estar criado, deve ser formalizada uma solicitação ao Gestor de Controle de Acesso do módulo/submódulo para que este, a partir do módulo de Controle de Acesso, faça a atribuição do perfil.

O módulo de Controle de Acesso está disponível no Portal SISAD e permite a atribuição de perfis por quatro critérios:

- Por usuário: perfil concedido individualmente a um usuário específico
- Por lotação: perfil concedido a todos os usuários lotados na unidade organizacional informada
- Por cargo: perfil concedido a todos os usuários que ocupem o cargo informado
- Por categoria: perfil concedido a todos os usuários que atendam os critérios da categoria[2] informada.

Uma vez concedido o perfil via módulo de Controle de Acesso, basta fazer novo login no módulo para que as atualizações de perfis concedidos sejam processadas e o usuário possa utilizá-los.

Critérios para Acesso do Perfil Auditor

O perfil Auditor ainda não está implementado no módulo Atualização Cadastral de Inativos e Pensionistas, mas entende-se que, de acordo com a explicação dada pela Auditora da CCAUD/CSJT em reunião do gtControleAcessoSIGEP, este perfil deve dar acesso de consulta a **todas** as telas do sistema.

Os perfis atuais do sistema e a previsão dos direitos a serem concedidos ao perfil Auditor podem ser consultados na planilha Mapa de Perfis de Acesso

[2] O módulo de Controle de Acesso permite a criação de categorias, pelos Regionais, que atendam às suas necessidades.

Autoatendimento (AA)

Procedimento e Critérios para Concessão de Acesso ao Módulo Autoatendimento (AA) e seus Submódulos

Procedimento para Concessão de Acesso

Para a concessão de acesso a perfis no módulo Autoatendimento e seus submódulos, o usuário precisa estar visível na mview IRH.MV_RH_PORTAL. A implementação desta view é feita na instalação do módulo nacional de Controle de Acesso em cada tribunal, conforme as instruções existentes da Wiki San-Doc (https://san-doc.csjt.jus.br/index.php/SIGEP-JT)

Após o usuário estar criado, deve ser formalizada uma solicitação ao Gestor de Controle de Acesso do módulo/submódulo para que este, a partir do módulo de Controle de Acesso, faça a atribuição do perfil.

O módulo de Controle de Acesso está disponível no Portal SISAD e permite a atribuição de perfis por quatro critérios:

- Por usuário: perfil concedido individualmente a um usuário específico;
- Por lotação: perfil concedido a todos os usuários lotados na unidade organizacional informada;
- Por cargo: perfil concedido a todos os usuários que ocupem o cargo informado;
- Por categoria: perfil concedido a todos os usuários que atendam os critérios da categoria[3] informada.

Uma vez concedido o perfil via módulo de Controle de Acesso, basta fazer novo login no módulo para que as atualizações de perfis concedidos sejam processadas e o usuário possa utilizá-lo.

Descrição dos critérios para Acesso do Perfil Auditor

O perfil Auditor ainda não está implementado no módulo de Autoatendimento, mas entende-se que, de acordo com a explicação dada pela Auditora da CCAUD/CSJT em reunião do gtControleAcessoSIGEP, este perfil deve dar acesso de consulta a **todas** as telas do sistema.

Os perfis atuais do sistema e a previsão dos direitos a serem concedidos ao perfil Auditor podem ser consultados na planilha Mapa de Perfis de Acesso

[3] O módulo de Controle de Acesso permite a criação de categorias, pelos tribunais, que atendam às suas necessidades.

Averbação de Capacitações (EJA)

Procedimento e Critérios para Concessão de Acesso ao Módulo Averbação de Capacitações (EJA)

Procedimento para Concessão de Acesso

Para a concessão de acesso a perfis no módulo Averbação de Capacitações, o usuário precisa estar visível na mview IRH.MV_RH_PORTAL. A implementação desta view é feita na instalação do módulo nacional de Controle de Acesso em cada tribunal, conforme as instruções existentes da Wiki San-Doc (https://san-doc.csjt.jus.br/index.php/SIGEP-JT).

Após o usuário estar criado, deve ser formalizada uma solicitação ao Gestor de Controle de Acesso do módulo/submódulo para que este, a partir do módulo de Controle de Acesso, faça a atribuição do perfil.

O módulo de Controle de Acesso está disponível no Portal SISAD e permite a atribuição de perfis por quatro critérios:

- Por usuário: perfil concedido individualmente a um usuário específico;
- Por lotação: perfil concedido a todos os usuários lotados na unidade organizacional informada;
- Por cargo: perfil concedido a todos os usuários que ocupem o cargo informado;
- Por categoria: perfil concedido a todos os usuários que atendam os critérios da categoria[4] informada.

Uma vez concedido o perfil via módulo de Controle de Acesso, basta fazer novo login no módulo para que as atualizações de perfis concedidos sejam processadas e o usuário possa utilizá-lo.

Critérios para Acesso do Perfil Auditor

O perfil Auditor ainda não está implementado no módulo Averbação de Capacitações, mas entende-se que, de acordo com a explicação dada pela Auditora da CCAUD/CSJT em reunião do gtControleAcessoSIGEP, este perfil deve dar acesso de consulta a **todas** as telas do sistema.

Os perfis atuais do sistema e a previsão dos direitos a serem concedidos ao perfil Auditor podem ser consultados na planilha Mapa de Perfis de Acesso.

[4] O módulo de Controle de Acesso permite a criação de categorias, pelos Regionais, que atendam às suas necessidades.

Conector eSocial SIGEP (CONN ESOCIAL)

Procedimento e Critérios para Concessão de Acesso ao Módulo Conector eSocial SIGEP (CONN ESOCIAL)

Procedimento para Concessão de Acesso

- O auditor precisa inicialmente de um acesso ao Keycloak, obtido através de um cadastro simples.
- Uma vez cadastrado, a equipe encarregada de conceder perfis no Keycloak deve atribuir ao auditor os seguintes perfis do cliente "sigep-esocial":
    - role_acesso_painel
    - role_acesso_cabecalho
    - role_acesso_detalhes
    - role_acesso_configuracoes
    - role_acesso_relatorios
    - role_acesso_consultas_extrator_sigep

Com esses perfis, o auditor terá capacidade de acessar todas as interfaces do sistema em modo leitura, sem permissão de escrita.

Critérios para Acesso do Perfil Auditor

O perfil Auditor é implementado dinamicamente no keycloak, logo, já pode ser aplicado ao auditor. De acordo com a explicação dada pela Auditora da CCAUD/CSJT em reunião do gtControleAcessoSIGEP, este perfil deve dar acesso de consulta a **todas** as telas do sistema.

Os perfis atuais do sistema e a previsão dos direitos a serem concedidos ao perfil Auditor podem ser consultados na planilha Mapa de Perfis de Acesso

Controle de Acesso (CAC)

Procedimento e Critérios para Concessão de Acesso ao Módulo Controle de Acesso (CAC)

Procedimento para Concessão de Acesso
Para a concessão de acesso a perfis no módulo Controle de Acesso, o usuário precisa estar visível na mview IRH.MV_RH_PORTAL. A implementação desta view é feita na instalação do módulo nacional de Controle de Acesso em cada Regional, conforme as instruções existentes da Wiki San-Doc.

Após o usuário estar criado, deve ser formalizada uma solicitação ao Gestor de Controle de Acesso do módulo/submódulo para que este, a partir do módulo de Controle de Acesso, faça a atribuição do perfil.

O módulo de Controle de Acesso está disponível no Portal SISAD e permite a atribuição de perfis por quatro critérios:

- Por usuário: perfil concedido individualmente a um usuário específico
- Por lotação: perfil concedido a todos os usuários lotados na unidade organizacional informada
- Por cargo: perfil concedido a todos os usuários que ocupem o cargo informado
- Por categoria: perfil concedido a todos os usuários que atendam os critérios da categoria[5] informada.

Uma vez concedido o perfil via módulo de Controle de Acesso, basta fazer novo login no módulo para que as atualizações de perfis concedidos sejam processadas e o usuário possa utilizá-las.

Critérios para Acesso do Perfil Auditor
O perfil Auditor ainda não está implementado no módulo Controle de Acesso, mas entende-se que, de acordo com a explicação dada pela Auditora da CCAUD/CSJT em reunião do gtControleAcessoSIGEP, este perfil deve dar acesso de consulta a **todas** as telas do sistema.

Os perfis atuais do sistema e a previsão dos direitos a serem concedidos ao perfil Auditor podem ser consultados na planilha Mapa de Perfis de Acesso

[5] O módulo de Controle de Acesso permite a criação de categorias, pelos Regionais, que atendam às suas necessidades.

Designação de Magistrados e Editais (DMAG)

Procedimento e Critérios para Concessão de Acesso ao Módulo Designação de Magistrados e Editais (DMAG)

Procedimento para Concessão de Acesso

O sistema é composto pelas seguintes soluções:

1. Editais: Sistema que permite a elaboração de editais de demanda para convocação automática de juízes substitutos;
2. Designação de Magistrados (DMAG): Sistema responsável por gerir as designações de magistrados.

Ambas soluções utilizam o keycloak para autenticação e controle de autenticação por perfis dinâmicos configurados nos próprios sistemas.

Atualmente o sistema só permite o acesso de usuário servidor/magistrado cadastrado no Módulo Principal do SIGEP-JT (srh2.servidor) e que possa ser autenticado pelo keycloak.

Configuração do Perfil Auditor

EDITAIS

Acessar o menu Gerencial → Gerenciar Permissões de Acesso.

Incluir novo perfil com nome “Auditor” e selecionar as seguintes permissões na aba Permissões:

- Permissão para emitir relatório de disponibilidade;
- Permissão para emitir relatório de lotação de juízes substitutos;
- Permissão para emitir relatórios de inscrições em editais;
- Permissão para visualizar editais.

Em seguida, na aba Vínculos, incluir em “Usuários Vinculados” o usuário que será utilizado pelo auditor.

Uma vez concedido o perfil, basta fazer novo login no módulo para que as atualizações de perfis concedidos sejam processadas.

DMAG

Acessar o menu Gerencial → Gerenciar Permissões de Acesso.

Incluir novo perfil com nome “Auditor” e selecionar na aba Permissões a permissão para gerenciar as designações de magistrados.

Em seguida, na aba Vínculos, incluir em “Selecionados” o usuário que será utilizado pelo auditor.

Uma vez concedido o perfil, basta fazer novo login no módulo para que as atualizações de perfis concedidos sejam processadas.

Critérios para Acesso do Perfil Auditor

O perfil Auditor pode ser configurado dinamicamente no DMAG e Editais. Podem ser vinculadas a este perfil quaisquer funcionalidades que julgarem necessárias para atuação do auditor.

Docência e Concursos de Magistrados (MAG)

Procedimento e Critérios para Concessão de Acesso ao Módulo Docência e Concursos de Magistrados (MAG)

Procedimento para Concessão de Acesso
Para a concessão de acesso a perfis no módulo MAG e seus submódulos, o usuário precisa estar visível na mview IRH.MV_RH_PORTAL. A implementação desta view é feita na instalação do módulo nacional de Controle de Acesso em cada Regional, conforme as instruções existentes da Wiki San-Doc.

Após o usuário estar criado, deve ser formalizada uma solicitação ao Gestor de Controle de Acesso do módulo/submódulo para que este, a partir do módulo de Controle de Acesso, faça a atribuição do perfil.

O módulo de Controle de Acesso está disponível no Portal SISAD e permite a atribuição de perfis por quatro critérios:

- Por usuário: perfil concedido individualmente a um usuário específico
- Por lotação: perfil concedido a todos os usuários lotados na unidade organizacional informada
- Por cargo: perfil concedido a todos os usuários que ocupem o cargo informado
- Por categoria: perfil concedido a todos os usuários que atendam os critérios da categoria[6] informada.

Uma vez concedido o perfil via módulo de Controle de Acesso, basta fazer novo login no módulo para que as atualizações de perfis concedidos sejam processadas e o usuário possa utilizá-los.

Critérios para Acesso do Perfil Auditor
O perfil Auditor ainda não está implementado no módulo MAG, mas entende-se que, de acordo com a explicação dada pela Auditora da CCAUD/CSJT em reunião do gtControleAcessoSIGEP, este perfil deve dar acesso de consulta a **todas** as telas do sistema.

Os perfis atuais do sistema e a previsão dos direitos a serem concedidos ao perfil Auditor podem ser consultados na planilha Mapa de Perfis de Acesso

[6] O módulo de Controle de Acesso permite a criação de categorias, pelos Regionais, que atendam às suas necessidades.

Folha de Pagamento (FOLHAWEB)

Procedimento e Critérios para Concessão de Acesso ao Módulo Folha de Pagamento (FOLHAWEB)

Procedimento para Concessão de Acesso
Para que um usuário possa receber acesso na FolhaWeb, ele deve estar cadastrado no Módulo Principal como um servidor e também no LDAP. Dessa forma a FolhaWeb armazena na sua base de dados o servidor, login e perfil, e assim gerencia as telas em que ele pode ter acesso.

A FolhaWeb disponibiliza os seguintes perfis:

- Usuário da Folha
- Consulta da Folha
- Super Usuário da Folha
- Gerente da Folha
- Usuário da TI
- Auditor da Folha

Dentre os perfis acima, apenas os perfis **Super Usuário da Folha** e **Usuário da TI** podem gerenciar a concessão de acessos.

Critérios para Acesso do Perfil Auditor
O perfil de Auditor já está implantado na FolhaWeb. Entretanto, pode passar por alguma revisão após as definições do gtControleAcessoSIGEP.

Os acessos que o perfil de Auditor possui podem ser consultados na planilha Mapa de Perfis de Acesso.

Gestão de Atos Administrativos (GAA)

Procedimento e Critérios para Concessão de Acesso ao Módulo Gestão de Atos Administrativos (GAA)

Procedimento para Concessão de Acesso

O GAA utiliza o keycloak para autenticação e o controle de autorização é feito por perfis dinâmicos configurado no próprio sistema.

Algumas funcionalidades são públicas dentro do contexto institucional e por isso não necessitam de concessão de permissão, por default os usuários autenticados terão acesso a visualização de atos vinculados a sua lotação.

Para que o usuário consiga autenticar é necessário que esteja cadastrado no Módulo Principal do SIGEP-JT (srh2.servidor) e que possa ser autenticado pelo keycloak (LDAP/AD)

Critérios para Acesso do Perfil Auditor
Podem ser vinculadas a este perfil quaisquer funcionalidades que julgarem necessárias para atuação do auditor.

Acessar o menu Gerencial → Permissões de Acesso.
Incluir novo perfil com nome “Auditor” e selecionar na aba Permissões as permissões que julgarem pertinentes

Em seguida, na aba Vínculos, incluir em “Selecionados” o usuário que será utilizado pelo auditor, nesta aba serão exibidos todos os usuários disponíveis para se autenticar no sistema de acordo com as regras já descritas em “Procedimentos para Concessão de Acesso”

Uma vez concedido o perfil, basta fazer novo login no módulo para que as atualizações de perfis concedidos sejam processadas.

Gestão de Estagiários (GEST)

Procedimento e Critérios para Concessão de Acesso ao Módulo Gestão de Estagiários (GEST)

Procedimento para Concessão de Acesso
Os usuários são mantidos pelo keycloak, geralmente se faz uma integração com o LDAP/AD e o keycloak já está com todos os usuários do LDAP/AD.

Em relação às permissões:

Atualmente o GEST possui hoje as seguintes roles:

- gest_estagiario
- gest_operador_rh
- gest_supervisor
- gest_suporte_ti
- gest_titular_unidade

Podemos dividir em 2 grupos.

As roles que devem ser atribuídas nominalmente para cada usuário:

- gest_operador_rh
- gest_suporte_ti
- gest_auditor (não implementado)

Essas 3 roles serão geridas totalmente dentro do Keycloak. As roles devem ser atribuídas nominalmente pois é uma informação que o sistema não consegue "deduzir" por conta própria.

Os passos para atribuir estão no manual de implantação:
https://san-doc.csjt.jus.br/index.php?title=SIGEP_1.26_-_Manual_de_Implanta%C3%A7%C3%A3o_-_Gest%C3%A3o_de_Estagi%C3%A1rios#PASSO_07_-_Configura%C3%A7%C3%A3o_do_keycloak

Atribuir a role gest_operador_rh para os usuários de RH

1. Acessar o item Users no menu lateral esquerdo
2. Buscar pelo nome do usuário
3. Clicar em Edit
4. Na aba Role Mappings
   4.1. selecionar o gest no campo Client Roles
   4.2. adicionar a role gest_operador_rh selecionando ela na lista a esquerda
   4.3. clicar em Add Selected

Repetir o passo acima para cada usuário do RH.

Atribuir a role gest_suporte_ti para os usuários de TI que vão dar suporte ao sistema (esse perfil acessa a tela de parâmetros e a tela de exceções)

Repete os mesmos passos do fluxo anterior, apenas alterando o passo 4.2:

- Adicionar a role gest_suporte_ti selecionando ela na lista a esquerda

Repetir o passo acima para cada usuário de suporte de TI.

Atribuir a role gest_auditor para os usuários de auditoria (esse perfil deve permitir a consulta em todas as telas do sistema)

Repete os mesmos passos do fluxo anterior, apenas alterando o passo 4.2:

- Adicionar a role gest_auditor selecionando ela na lista a esquerda

Repetir o passo acima para cada usuário de auditoria

As roles que são atribuídas automaticamente:

- gest_estagiario
- gest_supervisor
- est_titular_unidade

Essas 3 roles são atribuídas automaticamente no momento do login de acordo com os cadastros do sistema SIGEP e GEST. A gestão delas é automática.

Critérios para Acesso do Perfil Auditor

O perfil Auditor ainda não foi implementado no sistema GEST. Entretanto, segundo a explicação dada pela Auditora da CCAUD/CSJT em reunião do gtControleAcessoSIGEP, este perfil deve dar acesso de consulta a **todas** as telas do sistema.

Os perfis atuais do sistema e a previsão dos direitos a serem concedidos ao perfil Auditor podem ser consultados na planilha Mapa de Perfis de Acesso

Gestão de Passivos (MGP)

Procedimento e Critérios para Concessão de Acesso ao Módulo Gestão de Passivos (MGP)

O Módulo de Gestão de Passivos delega o controle de acessos ao módulo FolhaWeb. Já possuímos o mapa de acesso detalhado na planilha Mapa de Perfis de Acesso. Por este motivo, não existe nenhuma atividade específica do MGP para a concessão de acessos a auditores. Deve-se seguir os mesmos procedimentos descritos no documento relacionado ao Módulo FolhaWeb.

Gestão de Pessoas por Competências (PROGECOM)

Procedimento e Critérios para Concessão de Acesso ao Módulo Gestão de Pessoas por Competências (PROGECOM)

Procedimento para Concessão de Acesso

O acesso ao Módulo Principal deve ser realizado em duas etapas:

1. Cadastro do servidor através do menu do submódulo Gestão -> Cadastro -> Servidor;
2. Associação do servidor às roles através do submódulo SAO. Cada uma das roles (Cadastro, Consulta e Gerência) deve ser fornecida para o submódulo individualmente.
    2.1. Submódulos do framework SRH através do menu SIGEP - Privilégios -> Cadastro -> de Usuário;
    2.2. Submódulos do framework SAD através do menu Acesso - Privilégios -> Vinculação de Usuário a Módulo.

Critérios para Acesso do Perfil Auditor

Não há um perfil específico para Auditor implementado no Módulo Principal, mas como ficou definido pelo gtControleAcessoSIGEP que este perfil deverá permitir o acesso de consulta a todas as telas do sistema, o mesmo pode ser realizado seguindo o seguinte modelo:

- submódulos do framework SRH - O acesso de consulta pode ser realizado fornecendo os grants de RL_SRH_CONSULTA para cada um dos submódulos;
- submódulos do framework SAD - A role de consulta permite apenas a visualização de relatórios, enquanto as telas só podem ser acessadas por roles de gerência.

Módulo Principal (MP)

Procedimento e Critérios para Concessão de Acesso ao Módulo Módulo Principal (MP)

Procedimento para Concessão de Acesso

O acesso ao Módulo Principal deve ser realizado em duas etapas:

1. Cadastro do servidor através do menu do submódulo Gestão -> Cadastro -> Servidor;
2. Associação do servidor às roles através do submódulo SAO. Cada uma das roles (Cadastro, Consulta e Gerência) deve ser fornecida para o submódulo individualmente.
    2.1. Submódulos do framework SRH através do menu SIGEP - Privilégios -> Cadastro -> de Usuário;
    2.2. Submódulos do framework SAD através do menu Acesso - Privilégios -> Vinculação de Usuário a Módulo.

Critérios para Acesso do Perfil Auditor

Não há um perfil específico para Auditor implementado no Módulo Principal, mas como ficou definido pelo gtControleAcessoSIGEP que este perfil deverá permitir o acesso de consulta a todas as telas do sistema, o mesmo pode ser realizado seguindo o seguinte modelo:

- submódulos do framework SRH - O acesso de consulta pode ser realizado fornecendo os grants de RL_SRH_CONSULTA para cada um dos submódulos;
- submódulos do framework SAD - A role de consulta permite apenas a visualização de relatórios, enquanto as telas só podem ser acessadas por roles de gerência.

Pasta Funcional Eletrônica (SAF)

Procedimento e Critérios para Concessão de Acesso ao Módulo Pasta Funcional Eletrônica (SAF)

Procedimento para Concessão de Acesso
Os usuários são mantidos pelo Keycloak, geralmente se faz uma integração com o LDAP/AD e o Keycloak já está com todos os usuários do LDAP/AD.

Em relação às permissões:

Atualmente o SAF possui as seguintes roles:

- saf_consulta
- saf_administrador_grp
- saf_administrador_passivo_grp
- areatecnica

Podemos adicionar uma role.

- saf_auditor_grp (não implementado)

Essas 5 roles serão geridas dentro do Keycloak ou no LDAP/AD integrado ao KC. Não há gerenciamento de permissões dentro do sistema.

Critérios para Acesso do Perfil Auditor
O perfil Auditor ainda não foi implementado no sistema SAF. O novo perfil terá acesso de consulta a todos os assentamentos funcionais, semelhante ao perfil existente saf_consulta.

Os perfis atuais do sistema e a previsão dos direitos a serem concedidos ao perfil Auditor podem ser consultados na planilha Mapa de Perfis de Acesso.

Portal dos Sistemas Administrativos Nacionais (SISAD)

Procedimento e Critérios para Concessão de Acesso ao Módulo

Procedimento para Concessão de Acesso
Ao autenticar-se pelo keycloak, automaticamente é atribuído ao usuário conectado, o perfil "Usuário", que habilita a conexão ao Portal. Para os demais perfis especializados, deve ser formalizada uma solicitação ao Gestor Nacional do Portal para que este, a partir da tela "Atribuição de perfis de gestão", faça a atribuição do perfil.

A tela "Atribuição de perfis de gestão" está disponível no Portal SISAD e permite a atribuição de perfis somente para usuários individualmente.

Uma vez concedido o perfil, basta fazer novo login no módulo para que as atualizações de perfis concedidos sejam processadas e o usuário possa utilizá-los.

Critérios para Acesso do Perfil Auditor
O perfil Auditor ainda não está implementado no Portal SISAD, mas entende-se que, de acordo com a explicação dada pela Auditora da CCAUD/CSJT em reunião do gtControleAcessoSIGEP, este perfil deve dar acesso de consulta a **todas** as telas do sistema.

Os perfis atuais do sistema e a previsão dos direitos a serem concedidos ao perfil Auditor podem ser consultados na planilha Mapa de Perfis de Acesso

Requerimentos de Frequência Online (ROL)

Procedimento e Critérios para Concessão de Acesso ao Módulo Requerimentos de Frequência Online (ROL)

Procedimento para Concessão de Acesso
Para a concessão de acesso a perfis no módulo Requerimentos de Frequência Online, o usuário precisa estar visível na mview IRH.MV_RH_PORTAL. A implementação desta view é feita na instalação do módulo nacional de Controle de Acesso em cada Regional, conforme as instruções existentes da Wiki San-Doc.

Após o usuário estar criado, deve ser formalizada uma solicitação ao Gestor de Controle de Acesso do módulo/submódulo para que este, a partir do módulo de Controle de Acesso, faça a atribuição do perfil.

O módulo de Controle de Acesso está disponível no Portal SISAD e permite a atribuição de perfis por quatro critérios:

- Por usuário: perfil concedido individualmente a um usuário específico
- Por lotação: perfil concedido a todos os usuários lotados na unidade organizacional informada
- Por cargo: perfil concedido a todos os usuários que ocupem o cargo informado
- Por categoria: perfil concedido a todos os usuários que atendam os critérios da categoria[7] informada.

Uma vez concedido o perfil via módulo de Controle de Acesso, basta fazer novo login no módulo para que as atualizações de perfis concedidos sejam processadas e o usuário possa utilizá-los.

Critérios para Acesso do Perfil Auditor
O perfil Auditor ainda não está implementado no módulo Requerimentos de Frequência Online, mas entende-se que, de acordo com a explicação dada pela Auditora da CCAUD/CSJT em reunião do gtControleAcessoSIGEP, este perfil deve dar acesso de consulta a **todas** as telas do sistema.

Os perfis atuais do sistema e a previsão dos direitos a serem concedidos ao perfil Auditor podem ser consultados na planilha Mapa de Perfis de Acesso

[7] O módulo de Controle de Acesso permite a criação de categorias, pelos Regionais, que atendam às suas necessidades.

Sistema de Gestão de Escolas Judiciais (EJUD)

Procedimento e Critérios para Concessão de Acesso ao Módulo Sistema de Gestão de Escolas Judiciais (EJUD)

Procedimento para Concessão de Acesso

Para que um usuário possa receber acesso no SISEJUD, ele deve estar cadastrado no LDAP como um servidor interno ao Regional. Dessa forma o SISEJUD armazena na sua base de dados o servidor, login e perfil, e assim gerencia as telas em que ele pode ter acesso.

O SISEJUD disponibiliza o perfil de Administrador (escrito "Administrtador do Sistema" [sic]). Atualmente, todo o usuário interno que faz o login e não tem este perfil de Administrador tem o acesso de treinando (o qual permite apenas fazer inscrições).

Para conceder o acesso de auditor a um usuário (interno, como definido acima), deve-se fazer o login com um usuário que tenha o perfil de Administrador. Em seguida, acessar o menu Configurações / Acessos de usuário.

Sob “Lista de Usuários”, digitar um trecho do nome do usuário interno a quem se deseja conceder o acesso de Auditor e pressionar ENTER. Clicar no nome do usuário e clicar no botão Selecionar (item 1 da tela abaixo).

Em Grupos (item 2 da tela), aparecerá o novo perfil Auditor. Clicar em “Auditor” e clicar no botão Incluir.

Critérios para Acesso do Perfil Auditor

O perfil de Auditor ainda não está implementado no SISEJUD. Entretanto, pode passar por alguma revisão após as definições do gtControleAcessoSIGEP.

Os acessos que o perfil de Auditor deverá possuir podem ser consultados na planilha Mapa de Perfis de Acesso.

Sistema Integrado de Gestão em Saúde da Justiça do Trabalho (SIGS)

Procedimento e Critérios para Concessão de Acesso ao Módulo Sistema Integrado de Gestão em Saúde da Justiça do Trabalho (SIGS)

Procedimento para Concessão de Acesso

1. Disponibilizar acesso à rede interna do tribunal no keycloak.
2. Com o perfil Diretor (no SIGS):
    a. Cadastramento de terceirizado (Administração / Terceirizado) – Incluir ao menos as informações obrigatórias.
    b. Cadastramento de acesso – perfis (Administração / Configurações / Acesso) – Fornecer perfis (profissional de Saúde para acessar as informações relativas a cada área (ex: médico, psicólogo, assistente social, etc.)
        i. O auditor no SIGS deve ser um profissional da área de saúde.
    c. Cadastramento do Profissional (Administração / Profissional) – Incluir informações referentes ao Conselho, inscrição e UF).

Critérios para Acesso do Perfil Auditor

Foi decidido em reunião com o CSJT que para acessar informações protegidas pelo sigilo médico, os auditores terão que ser médicos para acessar informações médicas, psicólogo para acessar informações de psicologia e assim por diante.

Informações que não exigem sigilo médico devem ser acessadas através do perfil auditor pelo Diretor do Serviço de Saúde. Eventos e informações registradas na trilha de auditoria:

As trilhas de auditoria devem conter informações relacionadas minimamente aos seguintes tipos de eventos:

a) Quanto ao RES:

- Criação, consulta, acréscimo ou substituição de registros do RES;
- Importação e exportação de dados;
- Impressão de registros do RES.

b) Quanto às ações de usuário:

- Tentativas de autenticação de usuário, com ou sem sucesso;
- Troca de senha;
- Encerramento e bloqueio de sessão de usuário;
- Desbloqueio de sessão de usuário (aplicável apenas caso o S-RES permita o desbloqueio de sessões de usuário bloqueadas por inatividade);
- Realização de assinatura digital;
- Validação de assinatura digital;
- Aceitação do termo de concordância de uso (vide NGS1.12.01).

c) Quanto às ações operacionais:

- Conexão com o banco de dados;
- Atividades de configuração do sistema (por exemplo, parâmetros de configuração de senha, limite de tentativas de login e atribuição de permissão e/ou restrição de acesso a um prontuário por um profissional de saúde);
- Atividades de gerenciamento de usuários e papéis, incluindo inativação/bloqueio e ativação/desbloqueio de conta de usuário;
- Geração de senha para usuário;
- Acesso aos registros de auditoria;
- Realização e restauração de cópia de segurança;
- Erros relativos à execução de processos operacionais com respectiva descrição do erro (por exemplo, eventos de detecção de quebra de integridade em arquivos de cópias de segurança, conclusão de processos de exportação e importação, etc);
- Indisponibilidade de comunicação que impeçam a verificação da revogação do certificado digital (aplicável apenas para sistemas certificados para NGS2).

d) Quanto às interações entre sistemas (aplicável apenas em casos de comunicação entre S-RES):

- Envio e recepção de dados;
- Envio e recepção de confirmação de entrega de dados transmitidos;
- Erros de integridade e autenticação de mensagens;
- Erros de autenticação de parceiros.

e) Quanto às situações especiais:

- Ações de delegação de poder;
- Ações realizadas sob delegação de poder.

f) Com relação aos eventos citados acima, os registros de auditoria devem possuir, no mínimo, as seguintes informações para cada evento:

- Número de identificação única do registro da trilha;
- Data e hora do evento;
- Nível de criticidade (ex.: crítico, alerta, erro, informação, etc. Referência: RFC 5424);
- Tipo de evento;
- Identificação do componente gerador do evento (ex.: nome do componente, endereço IP, dispositivo do usuário, ponto de acesso, etc);
- Identificação do usuário gerador do evento, quando aplicável;
- Indicação de atividade realizada por delegação, quando aplicável;
- Identificador único e permanente do registro afetado pelo evento (por exemplo, identificador do sujeito da atenção).