CGU

CONTROLADORIA-GERAL DA UNIÃO
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

PROCESSO DE

GERENCIAMENTO DE ACESSO

SUBPROCESSO DE

GESTÃO DO CREDENCIAMENTO DE USUÁRIOS DE SISTEMAS

VERSÃO 1.0

março/2021

CONTROLADORIA-GERAL DA UNIÃO

SAS Quadra 01 Bloco A Edifício Darcy Ribeiro
70070-905 – Brasília-DF

Wagner de Campos Rosário
Ministro da Transparência e Controladoria-Geral da União

José Marcelo Castro de Carvalho
Secretário-Executivo

Valmir Gomes Dias
Ouvidor-Geral da União

Gilberto Waller Júnior
Corregedor-Geral da União

João Carlos Figueiredo Cardoso
Secretário de Combate à Corrupção

Antônio Carlos Bezerra Leonel
Secretário Federal de Controle Interno

Cláudia Taya
Secretária de Transparência e Prevenção da Corrupção

Henrique Aparecido da Rocha
Diretor de Tecnologia da Informação

Leonardo Alamy Martins
Coordenador-Geral de Infraestrutura Tecnológica

Equipe Técnica
Joyce Lustosa Belga
André Fonseca de Oliveira
Francisco Leonardo Lima Gazzola
Maura Paraíso Wanderley
Victor Diego Medeiros Lino
Vitor Picanço do Amaral

Brasília, março de 2021.

HISTÓRICO DE VERSÕES

Data	Versão	Descrição	Autor
06/2019	0.5	Elaboração do documento	Equipe Técnica
09/2019	0.7	Revisão e Aprovação para publicação	Gabinete/Diretor DTI
01/2020	1.0 beta	Atualização em função da publicação da Portaria CGU sobre Sistemas Estruturantes de Governo	Joyce Belga
03/2021	1.0	Atualização devido disponibilização da Solução de Consulta a Usuários Credenciados e migração do credenciamento para o Portal de Serviços	Joyce Belga

NOTA DA VERSÃO

Este subprocesso não abrange todos os sistemas em uso na CGU. Restringe-se àqueles sistemas de informação ativos no catálogo de serviços de TI do órgão, do tipo "serviços de negócio" e cujo acesso seja provido pela DTI. Dessa forma, softwares aplicativos ou sistemas do tipo "apoio técnico" ou, ainda, sistemas com acessos providos pelas próprias áreas de negócio não são contemplados neste subprocesso.

Logo, todas as referências a sistemas de informação neste documento restringem-se a esse escopo.

A lista de sistemas compreendidos por este subprocesso pode ser consultada na página da DTI na IntraCGU[1].

[1] https://cgugovbr.sharepoint.com/sites/intracgu-tecnologia-da-informacao/SitePages/Credenciamento-de-Usu%C3%A1rios-em-Sistemas.aspx (*http://intra.cgu.gov.br → Gestão Administrativa → Tecnologia da Informação → Sistemas → Credenciamento de Usuários*)

SUMÁRIO

1. INTRODUÇÃO

O credenciamento e o descredenciamento de usuários em sistemas referem-se a uma parte do gerenciamento de acesso, pela qual o usuário recebe as credenciais que permitirão acesso a determinado sistema de informação ou tem seu acesso retirado, em função de autorização prévia e da "necessidade de conhecer".

Este documento tem como objetivo apresentar as características deste subprocesso de Gestão do Credenciamento de Usuários de Sistemas, o qual integrará o **processo de Gerenciamento de Acesso**, e se alinhará ao **processo de Gerenciamento de Segurança da Informação**, a serem implantados no âmbito da Controladoria-Geral da União - CGU.

O documento está estruturado nos seguintes tópicos:

- Objetivo do Subprocesso;
- Benefícios Esperados;
- Referências;
- Definições;
- Políticas do Subprocesso;
- Papéis e Responsabilidades;
- Fluxo e Atividades do Subprocesso.

2. OBJETIVO DO SUBPROCESSO

O objetivo do subprocesso de Gestão do Credenciamento de Usuários de Sistemas pode ser descrito nos seguintes termos:

> *Gerenciar o credenciamento e o descredenciamento de usuários da CGU e de usuários externos quanto ao acesso aos sistemas de informação de uso necessário a este órgão – sejam de propriedade da CGU ou de outras instituições cujo acesso à CGU é autorizado, garantindo o acesso apenas dos usuários autorizados e impedindo o acesso dos demais usuários.*

3. BENEFÍCIOS ESPERADOS

São benefícios esperados com a implantação do subprocesso de Gestão do Credenciamento de Usuários de Sistemas no âmbito da DTI/CGU:

- Apoiar o Gerenciamento de Acesso a proteger a confidencialidade, a integridade e a disponibilidade dos sistemas de informação, pela garantia de que apenas usuários autorizados sejam capazes de acessar ou modificar esses sistemas;

- Proporcionar acesso adequado aos sistemas, bem como revogar direitos de acesso quando necessário, em tempo hábil, atendendo às necessidades do negócio, o que significa uma importante consideração de segurança da informação;

- Responder com mais eficiência e eficácia a solicitações de credenciamento/descredenciamento de sistemas, garantindo que os direitos que estão sendo fornecidos ou alterados, o sejam corretamente, uma vez que a legitimidade da solicitação é assegurada pela garantia do recebimento da autorização devida para que possa ser atendida;

- Executar rotinas de credenciamento/descredenciamento de forma mais controlada e em conformidade com os requisitos regulamentares pertinentes, principalmente no que tange aos sistemas estruturantes da Administração Pública Federal (APF).

4. REFERÊNCIAS

(1) Norma Complementar nº 03/IN04/SE/CGU, de 21 de outubro de 2016, que regulamenta os controles de acesso relativos à segurança da informação e comunicações no âmbito da CGU e dá outras providências;

(2) Norma Complementar nº 05/IN04/SE/CGU, de 03 de julho de 2017, que dispõe sobre a utilização dos recursos de tecnologia da informação da CGU;

(3) Norma Complementar nº 07/IN01/DSIC/GSIPR, de 15 de julho de 2014, que estabelece diretrizes para implementação de controles de acesso relativos à segurança da informação e comunicações;

(4) Norma Complementar nº 19/IN01/DSIC/GSIPR, de 15 de julho de 2014, que estabelece padrões mínimos de segurança da informação e comunicações para os sistemas estruturantes da administração pública federal;

(5) Portaria CGU nº 1.324, de 5 de abril de 2019, que institui a estrutura de governança para a gestão da Segurança Corporativa da CGU;

(6) Portaria CGU nº 1.420, de 16 de abril de 2019, que atualiza a Política de Governança de Tecnologia da Informação da Controladoria-Geral da União - PGTI/CGU;

(7) Portaria CGU nº 2.384, de 6 de outubro de 2020, que atualiza as Unidades Gestoras das Soluções de Tecnologia da Informação no âmbito da CGU;

(8) Portaria nº 2.042, de 22 de setembro de 2017, que Institui a Política de Segurança da Informação e das Comunicações na CGU;

(9) Tribunal de Contas da União, Boas Práticas em Segurança da Informação – 4ª edição – Brasília, 2012.

5. DEFINIÇÕES

No contexto deste subprocesso, são adotadas as definições a seguir:

TERMO	DEFINIÇÃO	FONTE
Acesso	Ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade.	NC03/IN04/SE/CGU
Agente Público	Todo aquele que exerce, ainda que transitoriamente, com ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função na CGU.	Portaria CGU nº 2042/2017

Auditoria	Inspeção e verificação formal para confirmar se uma norma ou um conjunto de orientações estão sendo seguidas, que os registros estão exatos ou que as metas de eficiência e eficácia estão sendo alcançadas. Uma auditoria pode ser conduzida por grupos internos ou externos.	NC21/IN01/DSIC /GSIPR
Autenticação	Processo de validação da identidade do usuário, que pode ser feito por diversos meios, tais como: combinação de usuário/senha, biometria ou utilização de certificado digital.	NC05/IN04/SE/ CGU
Autorização	Processo que visa garantir que as informações são acessíveis exclusivamente àqueles com permissão de acesso.	NC21/IN01/DSIC /GSIPR
Bloqueio de acesso	Processo que tem por finalidade suspender temporariamente o acesso.	NC03/IN04/SE/ CGU
Cadastrador parcial	Servidor do órgão, responsável pelo cadastramento e habilitação dos usuários nos Sistemas Estruturantes no respectivo âmbito organizacional.	Normas próprias dos sistemas estruturantes da APF
Catálogo de serviços	Conjunto de serviços que estão em homologação e em produção.	Processo de Gerenciamento do Catálogo de Serviços da CGU
Central de Serviços	Ponto único de contato entre os usuários e a Diretoria de Tecnologia da Informação para tratar requisições de serviço.	Processo de Central de Serviços de TI da CGU
Colaboradores	Fornecedores, estagiários e terceirizados alocados no órgão.	Portaria CGU nº 2042/2017
Controle de acesso lógico	O conjunto de procedimentos, recursos e meios utilizados com a finalidade proteger os ativos organizacionais baseados em tecnologia da informação contra acessos indevidos, bem como permitir acesso aos usuários legítimos desses ativos.	NC03/IN04/SE/ CGU
Credenciais ou Contas de acesso	Permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha.	NC03/IN04/SE/ CGU
Credenciamento	Processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer.	NC03/IN04/SE/ CGU
Direito ou nível de acesso	As configurações reais em que um usuário recebe acesso a um serviço ou grupo de serviços. Direitos típicos, ou níveis de acesso, incluem ler, escrever, executar, alterar, excluir.	ITIL
Exclusão de acesso	Processo que tem por finalidade suspender definitivamente o acesso, incluindo o cancelamento do código de identificação e do perfil de acesso.	NC03/IN04/SE/ CGU
Grupo designado	Conjunto de técnicos responsável por atender determinada requisição	Processo de Gerenciamento do Catálogo de Serviços da CGU
Necessidade de conhecer	Condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação.	NC03/IN04/SE/ CGU
Papel	Conjunto de responsabilidades, atividades e autoridades concedidas a uma pessoa ou equipe. Um papel é definido em um processo ou função. Uma pessoa ou equipe pode ter vários papéis; por exemplo, os papeis de gerenciador de configuração e gerente de mudança podem ser desempenhados por uma única pessoa.	ITIL

Perfil de acesso	Conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso.	NC03/IN04/SE/ CGU
Privilégio	Permissão de uso/acesso a um recurso de TI concedida a usuário ou grupos de usuários.	NC05/IN4/SE/ CGU
Serviços de apoio técnico	Serviços que suportam ou "sustentam" os serviços voltados para o cliente. Estes não são visíveis para o cliente, apenas pela área técnica de TI.	Processo de Gerenciamento do Catálogo de Serviços da CGU
Serviços de Negócio	Serviços de TI que são vistos pelo cliente. Estes serviços são serviços típicos que suportam os processos de unidade de negócio.	Processo de Gerenciamento do Catálogo de Serviços da CGU
Sistema Estruturante	Sistema com suporte de tecnologia da informação fundamental e imprescindível para planejamento, coordenação, execução, descentralização, delegação de competência, controle ou auditoria das ações do Estado, além de outras atividades auxiliares, desde que comum a dois ou mais órgãos da Administração e que necessitem de coordenação central.	NC19/IN01/DSIC /GSI/PR
Unidade gestora de solução de TI	Unidade organizacional responsável pela definição de processos de trabalho, requisitos, regras de negócio e níveis de serviço aplicáveis a uma solução de TI.	Portaria CGU nº 1420/2019
Usuário	Servidores ocupantes de cargo efetivo ou cargo em comissão e os ocupantes de emprego público, em exercício na CGU, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso à Rede CGU ou aos ativos de informação da CGU.	NC05/IN04/SE/ CGU

Cabe destacar que, ao longo do documento, não são referenciados os nomes dos produtos utilizados como soluções tecnológicas, dada sua natureza dinâmica e evolutiva. Todavia, no **Anexo II – Consultas operacionais** - é apresentada a correlação entre as soluções e o produto correspondente, com uso vigente na CGU. Dessa forma, por exemplo, é possível verificar que o produto sendo utilizado como ferramenta de gerenciamento de serviços de TI da CGU é o HP Service Manager – HPSM.

Todos os termos definidos nesta seção estão grafados em azul quando de sua utilização ao longo do documento.

6. POLÍTICAS DO SUBPROCESSO

Políticas são intenções e/ou expectativas gerenciais documentadas formalmente. São utilizadas para direcionar decisões e para garantir o desenvolvimento e a implementação consistente de processos, papeis e atividades.

A seguir são documentadas as políticas que orientam a execução do subprocesso de Gestão do Credenciamento de Usuários de Sistemas no âmbito da CGU:

POLÍTICA 01: Solicitação de acesso
Descrição
Há 3 possibilidades quanto à solicitação do usuário para que um acesso a um sistema de informação seja concedido, alterado ou revogado: • **Não requer solicitação**: há sistemas de informação em que não é necessário que o usuário solicite acesso, pois, ou possuem acesso aberto (sem necessidade de autenticação), ou o credenciamento é feito pelo próprio usuário (com autenticação), ou o acesso é concedido de maneira automática, conforme cargo, lotação ou outros critérios;

- **Solicitação diretamente à Unidade Gestora da Solução de TI**: há sistemas que possuem módulos específicos para credenciamento e descredenciamento habilitados para uso da Unidade Gestora da Solução de TI. Nesses casos, a solicitação é feita diretamente à Unidade Gestora, sobre a qual recai a responsabilidade pela criação e manutenção das contas de acesso;
- **Solicitação à Central de Serviços:** os demais sistemas, que requerem solicitação de acesso e cujo acesso não é provido diretamente pela Unidade Gestora da Solução de TI, necessitam que o usuário realize uma solicitação formal, por meio de um dos canais de atendimento da Central de Serviços.

Razão

Proporcionar maior gestão sobre as solicitações de acesso a sistemas que exigem controle de acesso, de forma que sejam registradas e, portanto, rastreáveis e mensuráveis.

Benefícios

- Obter maiores detalhes sobre a requisição efetuada, como, quando ocorreu, quem solicitou, quanto tempo levou para ser atendida, entre outras informações que possibilitam melhor gestão da solicitação;
- Conhecer e medir o volume de solicitações de acesso, para melhor dimensionar a equipe para atendimento;
- Maior padronização da forma de atendimento às solicitações de acesso, o que facilita o entendimento do processo pelos usuários e a interação entre esses e a DTI.

Informações complementares

- Neste subprocesso, conforme escopo explicitado na "Nota da Versão", apenas será tratada a modalidade de "Solicitação à Central de Serviços", que é por meio da qual as solicitações de acesso devem chegar para atendimento pela DTI. Dessa forma, todos os sistemas com acesso provido pela DTI devem ter sua solicitação registrada nos canais de atendimento da Central de Serviços, padronizando, assim, o canal de entrada das requisições.

POLÍTICA 02: Concessão de acesso

Descrição

É a concessão de acesso que permite ao usuário utilizar os sistemas de informação documentados no catálogo de serviços, conforme a autorização recebida.

Para utilizar determinados sistemas, pode ser necessário passar por procedimentos autorizativos de acesso, de forma a se verificar se o usuário está, de fato, qualificado para acessar o sistema, e, então, obter a autorização devida. Os procedimentos autorizativos são executados pelo **grupo autorizador** e poderão seguir um dos seguintes **fluxos de aprovação**:

- **Não tem:** não há procedimento autorizativo de acesso;
- **Aprovadores do grupo designado**: a solicitação de acesso é encaminhada para aprovação para um grupo determinado pelo Gestor da Solução;
- **Chefe ou substituto**: a solicitação de acesso é encaminhada para aprovação pela chefia do usuário (ou substituto);
- **Chefia e Gestor da Solução**: a solicitação de acesso é encaminhada para aprovação pela chefia do usuário, em seguida, para aprovação pelo Gestor da Solução;
- **Gestor da Solução**: a solicitação de acesso é encaminhada para aprovação pelo Gestor da Solução.

Se houver procedimentos autorizativos de acesso para o sistema, após a aprovação da solicitação pelo grupo autorizador, esta é encaminhada para concessão do acesso, efetivamente, pelo **grupo**

designado. Se não houver procedimentos autorizativos de acesso para o sistema, a solicitação é encaminhada diretamente para o grupo designado.

Uma vez que o usuário tenha o acesso concedido a um sistema de informação, ele terá as credenciais que o habilitam a utilizar o sistema com a autorização devida.

Razão

Sistematizar a concessão de acessos fazendo com que o acesso ao sistema se dê apenas por usuários devidamente credenciados, mediante procedimento autorizativo.

Benefícios

Evitar quebras de segurança da informação ao assegurar que apenas usuários legítimos e autorizados, foram qualificados para acessar o sistema de informação.

Informações complementares

- A depender do sistema, pode haver **requisitos adicionais de acesso** a serem exigidos para que o acesso seja concedido. Requisitos como dados pessoais ou funcionais, termo de responsabilidade, preenchimento de formulário, entre outros;
- Os procedimentos para concessão de acesso devem ser aplicados a todos os usuários, inclusive àqueles com privilégios (por exemplo, administradores), usuários internos e externos, para os casos normais ou emergenciais. Os **acessos privilegiados** devem ser bem monitorados e restritos a poucas pessoas, com a observância de rigorosos preceitos éticos e somente quando indispensável para a execução de atividade;
- É vedada a concessão de acesso para **colaboradores**, a sistema restrito por questões de sigilo, ou por ser diretamente vinculado a atividades típicas de controle, ou pelo perfil de acesso não ser compatível com as atividades inerentes ao respectivo objeto do instrumento que rege a contratação do profissional terceirizado ou disciplina o agenciamento dos estagiários, nos termos da legislação aplicável;
- A concessão de acesso deve observar as normas de **classificação de ativos de informação** e os dispositivos legais e regimentais relativos à confidencialidade e a outros critérios de classificação pertinentes, a fim de prover um nível adequado de proteção ao sistema, de acordo com a sua importância, sensibilidade e criticidade para a organização;
- As orientações para o usuário quanto a como é realizada a concessão de acesso a cada sistema de informação, conforme suas especificidades e requisitos exigidos, estão disponíveis no Portal de Serviços.

POLÍTICA 03: Alteração de acesso em função de eventos de pessoal

Descrição

À medida que os usuários trabalham na organização, seus papeis podem mudar e, portanto, suas necessidades de acessar sistemas também podem ser alteradas. Por isso, é necessário adaptar o(s) direito(s) de acesso do usuário que tenha mudado de atividades, a fim de readequar o acesso ao sistema. Ou seja, é necessário atualizar o(s) perfil(s) de acesso, concedendo novos e/ou revogando anteriores.

A seguir, alguns **eventos de pessoal** que podem implicar em alteração de acesso:

CATEGORIA DO EVENTO	EVENTO
Movimentação *(mudanças em que a necessidade de conhecer for decorrente do exercício do referido cargo, função ou unidade)*	Designação ou dispensa de cargo comissionado ou função de confiança
	Mudança de unidade ou lotação

Afastamento, licença ou penalidade *(usuário fora do órgão temporariamente)*	Afastamentos (para servir a outro órgão ou entidade, exercício de mandato eletivo, estudo ou missão no exterior, participação em programa de pós-graduação stricto sensu no país)
	Licenças que excedam o período de 1 ano (doença em pessoa da família, afastamento do cônjuge ou companheiro, atividade política, tratar de interesses particulares, desempenho de mandato classista)
	Envolvimento em inquérito penal, processo administrativo disciplinar (PAD) ou sindicância, decorrente de infrações cometidas no exercício das atribuições do cargo
Desligamento *(término do vínculo do usuário com o órgão)*	Aposentadoria
	Demissão
	Exoneração
	Falecimento
	Posse em cargo inacumulável
	Retorno para órgão de origem
	Encerramento de atividades, contrato ou acordo com colaboradores

Tabela 1 – eventos de pessoal que podem implicar em alteração de acesso

Os eventos de pessoal são registrados pela Unidade de Gestão de Pessoas[2], à exceção da "Mudança de unidade", a qual é registrada pelo próprio usuário, e do "Encerramento de atividades, contrato ou acordo com colaboradores", o qual é registrado pelo titular da unidade[3].

Quando o evento é registrado no sistema de informação que processa os eventos de pessoal, é executada uma rotina automática que descredencia o usuário de determinados sistemas. Nos eventos de movimentação, o descredenciamento é **parcial**, pois pode haver sistemas em que o descredenciamento não seja necessário, conforme definição do Gestor da Solução. Já nos eventos de afastamento e desligamento, o descredenciamento é **total**, pois são revogados todos os acessos do usuário nos sistemas de informação pertencentes ao escopo deste subprocesso[4].

Se o evento não for registrado no sistema de informação que processa os eventos de pessoal, o descredenciamento do usuário deve ser solicitado por meio da Central de Serviços. Em se tratando de concessão de novos acessos, decorrentes de alteração de acesso, para refletirem os privilégios necessários para desempenhar novas atribuições, esses serão solicitados pelo usuário, por meio da Central de Serviços, não sendo concedidos automaticamente pelo sistema de informação que processa eventos de pessoal[5].

[2] Norma Complementar nº 05/IN04/SE/CGU: *"A área de recursos humanos da CGU deve comunicar à DTI os desligamentos, as aposentadorias, os afastamentos e as movimentações de usuários que impliquem em mudanças de lotação, possibilitando a inativação e/ou atualização das contas de usuários para os privilégios necessários para o desempenho de suas funções na nova unidade*" (grifo nosso)

[3] Norma Complementar nº 05/IN04/SE/CGU: *"A criação de conta de usuário para profissionais de empresas contratadas, estagiários, consultores e afins, com objetivo de acesso a soluções de tecnologia da informação (TI) disponibilizadas na Rede CGU, deve ser solicitada à DTI pelo titular da unidade onde serão executadas as atividades, e deve ser precedida de cadastramento do usuário na Rede CGU e de assinatura do Termo de Responsabilidade. Cessado o motivo da concessão do acesso, o titular da unidade deverá requerer a imediata revogação do acesso à DTI."* (grifo nosso)

[4] Até o momento da publicação desta versão do documento (1.0), os eventos da categoria "movimentação" não eram registrados pelo sistema, tampouco gerados automaticamente os tickets para descredenciamento parcial. Também, para os eventos das categorias de "afastamento, licença ou penalidade" e "desligamento" realizados pelo sistema, era realizado apenas descredenciamento parcial (e não total - de todos os sistemas cadastrados pela DTI). Veja os detalhes no **Anexo III – Automação de descredenciamentos em alteração de acessos.**

[5] Norma Complementar nº 05/IN04/SE/CGU: *"Quando da mudança de lotação, as permissões concedidas serão atualizadas para refletirem os direitos e privilégios necessários para desempenhar as funções na nova lotação. Neste caso, as permissões especiais deste usuário serão excluídas e, caso ainda exista a necessidade de acesso, deverão ser novamente solicitadas*" (grifo nosso)

Dessa forma, em resumo, tem-se que a alteração de acesso decorrente de eventos de pessoal pode ser iniciada de 2 modos:

- **Pelo sistema de informação que processa eventos de pessoal**: iniciada automaticamente, no momento da alteração do cadastro do usuário neste sistema, quando, então, o próprio sistema abrirá um ticket na ferramenta de gerenciamento de serviços de TI da CGU, para descredenciar o usuário imediatamente, naqueles sistemas em que houver necessidade de revogação;
- **Pela Central de Serviços**: iniciada a partir de solicitação direta do responsável, por meio de um dos canais de atendimento da Central de Serviços, a fim de descredenciá-lo do antigo perfil de acesso ao sistema ou credenciá-lo no novo perfil de acesso ao sistema.

Razão

Gerenciar as alterações nos requisitos de acesso de um usuário a um sistema de informação.

Benefícios

Ciência em tempo hábil dos eventos de pessoal que impliquem em mudanças de acesso, de forma que as alterações possam ser realizadas de maneira tempestiva, principalmente no que se refere a restrições de acesso de usuários não mais autorizados.

Informações complementares

As alterações de acesso decorrentes de eventos de pessoal que atualmente são iniciadas pela Central de Serviços serão implementadas, gradativamente e mediante avaliação do esforço pela DTI, no sistema que processa eventos de pessoal, para possibilitar, futuramente, que tais alterações relacionadas ao ciclo de vida típico do usuário sejam todas iniciadas por este sistema.

POLÍTICA 04: Revogação de acesso

Descrição

A revogação de acesso remove o(s) acesso(s) do usuário, o descredenciando para utilização de determinado(s) perfil(s) de acesso ao sistema.

A solicitação de descredenciamento deverá ser providenciada quando cessada a "necessidade de conhecer" do usuário e nos demais casos em que se fizer necessária (conforme **tabela 1** de eventos de pessoal que podem implicar em alteração de acesso).

Razão

Impedir acessos de usuários não mais autorizados, observando os princípios da "necessidade de conhecer" e do privilégio mínimo.

Benefícios

Evitar quebras de segurança da informação advindas de ações (intencionais ou não) de usuários não mais autorizados.

Informações complementares

- Para os sistemas de informação que dispõem da funcionalidade de **bloqueio de acesso**, a qual permite suspender temporariamente o acesso do usuário, esta poderá ser utilizada para os eventos de afastamento temporário do usuário (conforme **tabela 1** de eventos de pessoal que podem implicar em alteração de acesso);
- A **DTI** poderá revogar acessos, sem aviso prévio, a fim de coletar evidências ou minimizar os riscos à segurança da informação e comunicações, diante de suspeitas de violação do disposto na Política de Segurança e demais normas, para evitar danos ou comprometimento dos sistemas de informação;
- A revogação de acesso de **colaboradores** deve ser cuidadosamente tratada a fim de garantir que seus perfis de acesso sejam imediatamente removidos quando não mais justificados, tendo prazo

de validade máximo igual ao período de vigência do contrato ou período de duração de suas atividades.

POLÍTICA 05: Revisão de acessos
Descrição
A revisão de acessos permite realizar uma análise crítica periódica dos acessos ativos, de forma a assegurar que estejam compatíveis com as reais necessidades do usuário, identificando não conformidades e providenciando as adequações necessárias. A revisão de acessos deverá ser realizada no mínimo **anualmente** pelos Gestores de Solução. A DTI, com essa periodicidade ou sob demanda, proverá aos Gestores de Solução, a lista de usuários com acessos ao(s) sistema(s) sob sua gestão, para que este a avalie em busca de acessos indevidos. Se houver, o Gestor da Solução deverá solicitar, por meio dos canais de atendimento da Central de Serviços, as revogações necessárias.
Razão
Verificar os direitos de acesso para garantir que os acessos ativos estejam apropriados e acessos obsoletos ou indevidos sejam removidos.
Benefícios
Proporcionar maior confiabilidade e segurança quanto à correição dos perfis de acesso atribuídos.
Informações complementares
• O gestor da solução, quando da revisão de acessos, deve atentar, especialmente, para aqueles direitos de acessos **privilegiados**, pois esses podem representar um risco significativo, uma vez que possuem acesso para modificação de informações na maioria das funcionalidades do sistema; • A regra geral de revisão de acessos não invalida regras próprias já existentes em alguns sistemas, as quais devem permanecer respeitadas.

POLÍTICA 06: Sistemas Estruturantes da APF
Descrição
O acesso aos sistemas estruturantes da APF será concedido, alterado ou revogado em conformidade com as políticas e os normativos específicos que disciplinam o uso, os controles e os perfis de acesso de cada sistema estruturante, quando houver; e de acordo com a Portaria CGU que define os critérios e os procedimentos para acesso dos usuários do órgão a esses sistemas.
Razão
Disciplinar os controles e o acesso aos sistemas estruturantes da APF, bem como atender aos padrões mínimos de segurança da informação e comunicações estabelecidos para esses sistemas.
Benefícios
• Minimizar falhas, proporcionando maior segurança, qualidade e padronização nos acessos concedidos, alterados e revogados nos sistemas estruturantes da APF; • Assegurar conformidade com os requisitos regulamentares pertinentes.
Informações complementares
• A concessão de perfis de acesso aos sistemas estruturantes é baseada nas atribuições funcionais do usuário mediante o sistema; • A concessão de acesso a todos os sistemas estruturantes deve ser aprovada previamente por grupo autorizador, antes da operacionalização pelo grupo designado;

- Para os sistemas estruturantes da APF, o grupo designado corresponderá ao(s) Cadastrador(s) Parcial(s) indicado pelo interlocutor do sistema estruturante.

POLÍTICA 07: Consulta usuários credenciados
Descrição
A Solução de consulta aos usuários credenciados, disponível para todos os sistemas escopo deste subprocesso, possibilita a realização de 2 pesquisas: • **Por usuário**: permite visualizar os sistemas que um determinado usuário acessa, com respectivos perfis de acesso; • **Por sistema**: permite visualizar os usuários que acessam um determinado sistema, com respectivos perfis de acesso. A Solução será utilizada pela equipe de atendimento ao usuário, ao receber solicitações de revogação ou de revisão de acessos, para que possa, então, providenciar o descredenciamento do usuário.
Razão
Possibilitar o conhecimento dos direitos de acesso vigentes do usuário, de forma centralizada, a fim de subsidiar a revisão de acessos e as demais requisições de descredenciamento.
Benefícios
Maior facilidade, confiabilidade e agilidade para efetuar descredenciamentos.
Informações complementares
• A Solução de consulta aos usuários credenciados está disponível para a equipe de atendimento ao usuário; • A Solução de consulta aos usuários credenciados não permite verificar direitos de acessos revogados do usuário, mas somente visualizar direitos de acessos ativos; • Além da Solução de consulta a usuários credenciados, alguns sistemas, por funcionalidades próprias dos mesmos, podem disponibilizar essa função internamente.

7. PAPÉIS E RESPONSABILIDADES

Um papel é um conjunto de responsabilidades, atividades e autoridades definidas em um processo e atribuídas a uma pessoa, equipe ou função. A seguir são apresentados os papeis envolvidos no subprocesso de Gestão do Credenciamento de Usuários de Sistemas proposto para a DTI:

GERENTE DO CREDENCIAMENTO DE USUÁRIOS DE SISTEMAS
Perfil
São competências requeridas para este perfil: • Conhecimentos e experiência em Gerenciamento de Serviços de TI, especialmente quanto a gestão dos processos de gerenciamento de segurança da informação e gerenciamento de acesso, conforme boas práticas ITIL; • Capacidade analítica para tomar decisões e propor melhorias no âmbito da gestão do subprocesso de credenciamento de usuários em sistemas e de seu relacionamento, principalmente, com os processos de gerenciamento de segurança da informação e gerenciamento de acesso; • Habilidade de negociação para obter consenso e colaboração entre as diferentes áreas da CGU. Recomenda-se que esse papel seja exercido por servidor público do quadro permanente da CGU, visto as atividades de gestão associadas e a necessidade de lidar com equipes terceirizadas.

Obs.: O ITIL, biblioteca internacional de boas práticas em gerenciamento de serviços de TI, indica que não deve haver um gerente especificamente para o subprocesso de credenciamento de usuários em sistemas, mas que este pode ser um papel exercido pelo Gerente de Segurança da Informação, haja vista que é o processo de Gerenciamento de Segurança da Informação que define e mantém os processos e as políticas relacionadas. Todavia, como esse processo de Gerenciamento de Segurança não está formalizado na CGU, será indicado um gerente específico para o subprocesso de credenciamento[6].

Objetivos

Gerenciar a execução do subprocesso de Gestão do Credenciamento de Usuários de Sistemas.

Tarefas/Atividades

Constituem atividades e tarefas do Gerente, para fins do disposto neste subprocesso:

- Monitorar a execução do subprocesso;
- Aferir os indicadores de desempenho do subprocesso;
- Elaborar e divulgar relatórios de desempenho da execução do subprocesso;
- Analisar e validar solicitações de modificações no subprocesso;
- Realizar os ajustes necessários referentes às solicitações de mudanças no subprocesso;
- Manter o registro de melhorias do subprocesso.

Responsabilidades

Além das competências gerais atribuídas aos gerentes de processo da CGU, conforme Portaria nº 3.091/2018, o gerente deste subprocesso também tem a responsabilidade de:

- Facilitar a introdução e adaptação ao subprocesso e gerenciar a execução durante o ciclo de vida;
- Buscar a qualidade, a eficiência e a efetividade gerais do subprocesso;
- Manter o subprocesso atualizado para que esteja adequado aos propósitos da organização;
- Administrar impasses durante a execução do subprocesso;
- Administrar os recursos envolvidos na execução das tarefas do subprocesso;
- Promover o uso de procedimentos padronizados para execução das atividades do subprocesso;
- Apoiar os demais papeis na execução de suas atividades e responsabilidades;
- Deliberar sobre a escolha e utilização de ferramentas para automação do subprocesso;
- Conscientizar os envolvidos da importância do subprocesso;
- Coordenar interfaces entre o subprocesso e o processo de gerenciamento de acesso, bem como com os outros processos de gerenciamento de serviços de TI, para garantir uma abordagem integrada (principalmente em relação aos processos de gerenciamento de segurança da informação, gerenciamento de catálogo de serviços, cumprimento de requisição e central de serviços de TI);
- Garantir que os mecanismos automatizados de concessão/revogação de acessos estejam funcionando em conformidade com este subprocesso.

GESTOR DA SOLUÇÃO

Perfil

Servidor da Unidade Gestora da Solução de TI, responsável pela gestão da solução que automatiza processos de trabalho sob sua responsabilidade. Possui conhecimento negocial sobre o sistema de informação que gere.

Objetivos

Ser o responsável negocial do sistema, definindo e revisando as regras de acesso ao seu sistema. Deve ser consultado e comunicado sobre quaisquer modificações nessas regras.

[6] Até a indicação do Gerente específico para o Subprocesso de Credenciamento, este papel será exercido pelo Serviço de Atendimento ao Usuário (SEATE/CGTEC/DTI/SE).

Tarefas/Atividades
• Definir os privilégios, perfis e direitos de acesso de usuários às funcionalidades e às informações disponibilizadas pelo sistema, bem como as regras de concessão e de revogação de acesso; • Definir os procedimentos autorizativos para acesso ao(s) sistema(s) sob sua gestão, especificando, quando necessário, o fluxo de aprovação e o grupo autorizador; • Definir o grupo designado para atendimento de solicitações de acesso; • Revisar periodicamente os acessos ao sistema, procedendo a uma análise crítica da lista de usuários do sistema e solicitando a alteração de acessos, caso necessário.
Responsabilidades/ Autoridades
• Participar da tomada de decisões relativas aos acessos do(s) sistema(s) sob sua gestão; • Zelar pela base de usuários do sistema sob sua gestão, incluindo usuários externos e colaboradores, para que somente pessoas autorizadas tenham acesso; • Determinar, em conjunto com o gerente do subprocesso, regras apropriadas para concessão, alteração e revogação de acessos ao(s) sistema(s) sob sua gestão, com os requisitos e o rigor de controles necessários para garantir a segurança dos ativos sob sua responsabilidade; • Solicitar modificações nos procedimentos de acesso relacionados ao(s) sistema(s) sob sua gestão; • Efetuar os procedimentos de concessão, alteração e revogação de acessos no(s) sistema(s) sob sua gestão, nos casos em que a solicitação de acesso é feita diretamente a Unidade Gestora da Solução de TI; • Responder à revisão de acessos, quando solicitado pela DTI.

GRUPO AUTORIZADOR
Perfil
Pessoas que realizam os procedimentos autorizativos de acesso dos sistemas que os exigem, sendo responsáveis por prover a autorização, conforme fluxo de aprovação definido pela Unidade Gestora da Solução de TI. Podem compor o grupo autorizador: a chefia imediata (ou substituto) e/ou o Gestor da Solução ou, ainda, um conjunto de pessoas nomeado como “aprovadores do grupo designado”.
Objetivos
Aprovar o credenciamento/descredenciamento do usuário em um sistema de informação.
Tarefas/Atividades
Autorizar a execução da concessão ou revogação do acesso solicitado.
Responsabilidades
Avaliar se o nível de acesso a ser concedido ao usuário é adequado e apropriado aos propósitos do negócio e à execução dos trabalhos, bem como se está consistente com a política de segurança de informação e demais normativos aplicáveis.

GRUPO DESIGNADO
Perfil
Equipe técnica que operacionalizará, de fato, o acesso do usuário após o recebimento da aprovação devida, se houver. Pertence à fila de responsáveis pelo atendimento da requisição. Essa equipe pode estar em qualquer área da CGU – finalística ou DTI -, ou, ainda, pode ser um procedimento automático (por exemplo, executado via ferramenta de orquestração).
Objetivos
Atender à solicitação de acesso.
Tarefas/Atividades
• Conferir os requisitos adicionais de acesso, se houver essa exigência no sistema;

- Prover o direito requerido na solicitação de concessão de acesso;
- Remover ou restringir o direito requerido na solicitação de revogação de acesso.

Responsabilidades/ Autoridades

Prover condição operacional de acesso ao sistema de informação.

USUÁRIO

Perfil

Agente público ou colaborador que utiliza sistema(s) de informação necessário(s) ao trabalho da CGU. O usuário pode ser interno (em exercício na CGU) ou externo (de outro órgão/entidade, mas que obteve autorização para acesso a um sistema de informação da CGU).

Objetivos

Viabilizar a consecução de suas atividades de trabalho, conforme sua atribuição organizacional.

Tarefas/Atividades

- Solicitar concessão, alteração ou revogação de acesso a um determinado sistema, conforme responsabilidades constantes na **tabela 1** - eventos de pessoal que podem implicar em alteração de acesso;
- Fornecer requisitos adicionais de acesso, se assim o for exigido pelo sistema, como dados pessoais ou funcionais, termo de responsabilidade, preenchimento de formulário, etc.

Responsabilidades

- Fazer uso do(s) perfil(s) de acesso recebido(s) única e exclusivamente em razão do exercício da função pública e para os fins que lhe foi designado, cumprindo as regras e requisitos estabelecidos na política de segurança e demais normas relacionadas;
- Manter sigilo de sua credencial de acesso, que é pessoal e intransferível, e das informações obtidas por meio do perfil concedido para acesso ao sistema;
- Cuidar da integridade, confidencialidade e disponibilidade de dados e informações do sistema de informação que acessa, devendo comunicar quaisquer irregularidades, falhas, anormalidades ou violações identificadas.

CENTRAL DE SERVIÇOS

Perfil

A central de serviços é o canal para o usuário registrar uma requisição de serviço para a DTI. São competências requeridas para o perfil de atendente da central de serviços, conforme o processo da central de serviços:

- Profissional com experiência em TI, em particular microinformática e rede de computadores;
- Possuir boa habilidade em comunicação verbal e escrita;
- Habilidade para lidar com os usuários de maneira cordial e profissional;
- Ser orientado ao cliente e suas necessidades.

Objetivos

Realizar o atendimento do usuário quanto a solicitação de acesso (concessão, revogação, alteração ou revisão), satisfazendo suas necessidades e cumprindo os padrões de qualidade.

Tarefas/Atividades

- Realizar tarefas/atividades seguindo as políticas dos processos da Central de Serviços e do Cumprimento de Requisição, os quais envolvem o registro, a categorização, o atendimento e o encerramento da solicitação, entre outros, que impactam diretamente na solicitação de acesso.
    - Por exemplo, é a adequada categorização da requisição pelo atendente da central de serviços que determina o encaminhamento (automático) da solicitação para análise do grupo autorizador, se houver, ou para atendimento pelo grupo designado;

- Conceder/revogar direitos de acesso a sistemas “simples”, os quais não possuem procedimentos autorizativos de acesso, sendo este concedido/revogado diretamente por grupo designado que está na Central de Serviços[7];
- Gerar a lista de usuários que acessam um determinado sistema, valendo-se da solução de consulta a usuários credenciados, para apoiar a revisão de acessos, anualmente ou quando assim for solicitado pelo Gestor da Solução (*);
- Gerar a lista de sistemas acessados por um determinado usuário, valendo-se da solução de consulta a usuários credenciados, para apoiar a revogação de acessos, quando assim for solicitado (*);

OBS: As atividades sinalizadas com (*) serão executadas exclusivamente pela Equipe de Atendimento ao Usuário da DTI.

OBS: A forma como a Central de Serviços poderá realizar consultas operacionais às informações necessárias para o desempenho de suas atividades está detalhada no **Anexo II - Consultas operacionais** - deste documento.

Responsabilidades/ Autoridades

- Comunicar com o usuário para garantir que ele saiba quando a solicitação de acesso foi atendida e, se não o for, por quais motivos, bem como garantir que ele receba qualquer outro suporte necessário;
- Relatar incidentes que tenha observado relacionados ao acesso (por exemplo, usuários tentando acessar sistemas sem autoridade; ou usuários relatando incidentes que indicam que um sistema foi usado de forma inadequada, como, por um ex-funcionário que usou um nome de usuário antigo para obter acesso e fazer alterações não autorizadas).

OBS: É incomum que a Central de Serviços tenha uma pessoa dedicada para gerenciar o credenciamento, mas o gerente da Central de Serviços garantirá que os procedimentos apropriados sejam definidos e executados de acordo com os requisitos do processo e da política.

RACI

A matriz RACI é um método utilizado para definir os papéis e responsabilidades dos atores envolvidos em um processo. RACI é um acrônimo em inglês para:

- **Responsible** (Responsável):
  - Pessoa, função ou unidade organizacional responsável pela execução de uma atividade no âmbito de um processo.
- **Accountable** (Responsabilizado):
  - É o dono da atividade.
  - Deverá fornecer os meios para que a atividade possa ser executada.
  - Será responsabilizado caso a atividade não alcance os seus objetivos.
  - Cada atividade só pode possuir um Accountable.
- **Consulted** (Consultado):
  - Pessoas que deverão ser consultadas durante a execução da atividade.
  - As informações levantadas junto a essas pessoas tornam-se entradas para a execução da atividade.
- **Informed** (Informado):
  - Pessoas que serão informadas acerca do progresso da execução da atividade.

[7] O Gestor da Solução é questionado, durante o processo de Gerência de Liberação, se o cadastramento no sistema pode ser realizado por terceirizados (Central de Serviços).

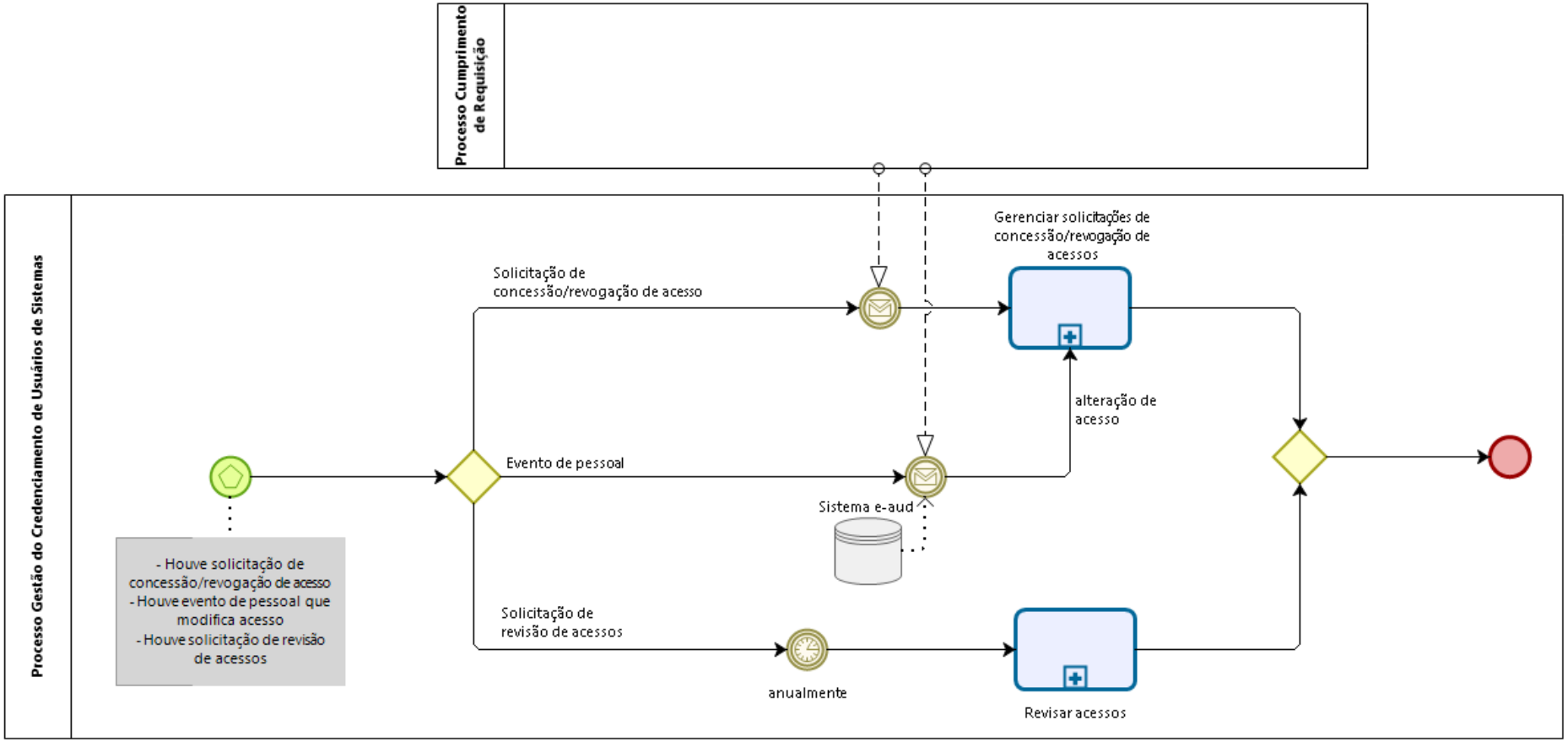
A matriz RACI a seguir documenta a relação existente entre as atividades do subprocesso e os papéis envolvidos na execução dessas.

ATIVIDADE	GESTOR DA SOLUÇÃO	GRUPO AUTORIZADOR	GRUPO DESIGNADO	USUÁRIO	CENTRAL DE SERVIÇOS
Realizar verificações				C/I	R/A
Prover direitos		C	R/A	C/I	
Remover ou restringir direitos		C	R/A	C/I	
Gerar lista de usuários que acessam o(s) sistema(s)	C/I				R/A
Analisar criticamente a lista de usuários do sistema	R/A				C/I

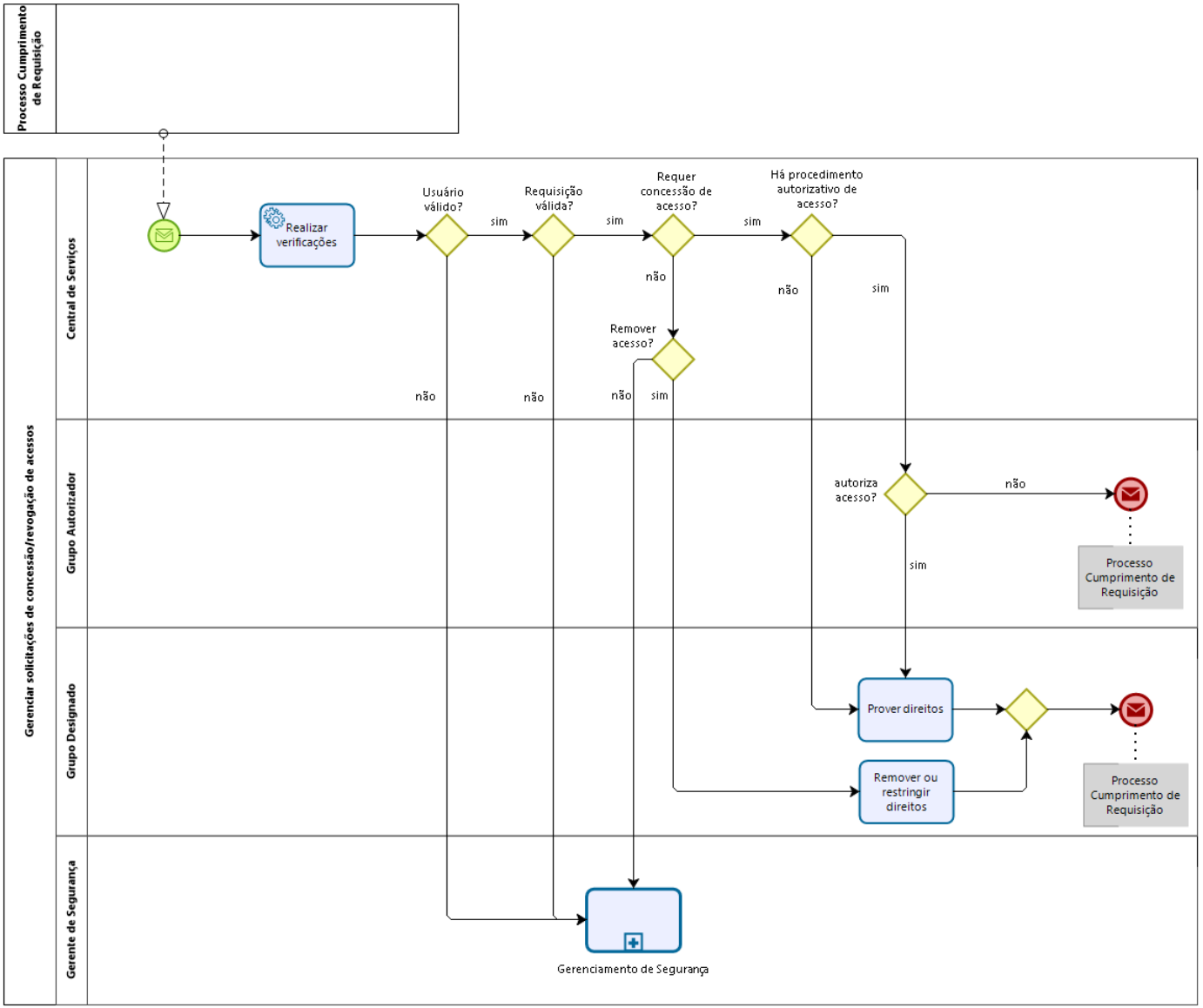
Responsável – R; Responsabilizado- A; Consultado – C; Informado – I.

8. FLUXO E ATIVIDADES DO SUBPROCESSO

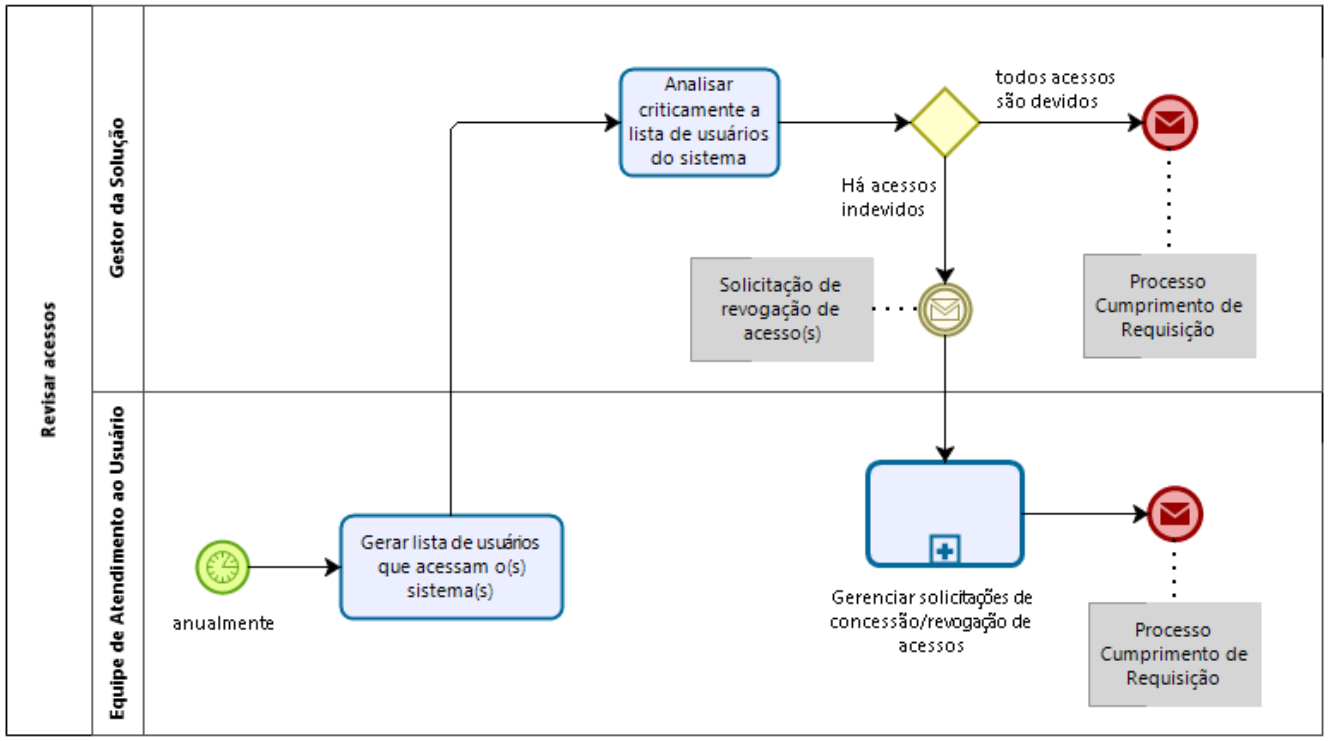
Fluxo macro da Gestão do Credenciamento de Usuários de Sistemas:



Fluxo detalhado - Gerenciar solicitações de concessão/revogação de acessos:



Fluxo detalhado - Revisar acessos:



A seguir são detalhadas as atividades integrantes da Gestão do Credenciamento de Usuários de Sistemas:

Realizar verificações
Objetivo
Verificar a solicitação de acesso quanto a identidade do usuário e quanto a qualificação para acesso.
Início
Ao registrar o chamado *(atividade do processo da Central de Serviços).*
Entradas
Solicitação de acesso a um sistema.
Saídas
Solicitação de acesso a um sistema verificada.
Descrição das tarefas e fluxos de informação
Essa tarefa é executada automaticamente pela ferramenta de gerenciamento de serviços de TI da CGU, a qual apenas disponibiliza a possibilidade de registro de requisições para usuários válidos.
Descrição detalhada da atividade
-

Prover direitos
Objetivo
Fornecer ao usuário os direitos para utilizar o sistema solicitado.
Início
Após a verificação de acesso realizada para uma solicitação de concessão de acesso.
Entradas
Solicitação de concessão de acesso a um sistema verificada.
Saídas
Acesso ao sistema concedido.
Descrição das tarefas e fluxos de informação
Se houver procedimentos autorizativos para acesso ao sistema, o grupo autorizador fará a análise e posterior aprovação, se o acesso for pertinente. Em seguida, o grupo designado proverá o direito devido. Se não houver procedimento autorizativo para acesso ao sistema, o grupo designado proverá o direito devido ao sistema.
Descrição detalhada da atividade
-

Remover ou restringir direitos
Objetivo
Revogar o(s) direito(s) de acesso do usuário ao sistema.
Início
Após a verificação de acesso realizada para uma solicitação de revogação de acesso.
Entradas
Solicitação de revogação de acesso a um sistema verificada.
Saídas
Acesso ao sistema revogado.
Descrição das tarefas e fluxos de informação
A solicitação de remoção/restrição de direitos pode ocorrer a partir de uma requisição cadastrada pelo solicitante diretamente na ferramenta de gestão de serviços de TI da CGU ou pode ser gerada, nesta mesma ferramenta, a partir de uma alteração no cadastro do usuário no sistema que processa eventos de pessoal. Nesse último caso, o sistema abre automaticamente um ticket na ferramenta de gestão de serviços de TI da CGU requerendo a remoção dos direitos de acesso devidos do usuário.

A partir de então, se houver procedimentos autorizativos para revogação do acesso, o grupo autorizador fará a análise e posterior aprovação, se pertinente. Em seguida, o grupo designado removerá o(s) direito solicitado(s). Se não houver procedimento autorizativo para revogação de acesso no sistema, o grupo designado removerá o(s) direito(s) de acesso ao sistema. Antes de proceder ao descredenciamento do usuário, pode ser que o Gestor da Solução solicite[8] a lista de sistemas que o usuário acessa, para avaliar em quais perfis e sistemas o usuário deverá ter seu acesso removido. Nesse caso, a equipe de atendimento ao usuário da DTI verificará a solução de consulta de usuários credenciados e repassará a informação ao Gestor da Solução.
Descrição detalhada da atividade
–

Gerar lista de usuários que acessam o sistema
Objetivo
Prover informação sobre os usuários ativos no sistema para que o Gestor da Solução possa validá-la.
Início
Em data fixa, anualmente.
Entradas
Agendamento anual da revisão de acessos.
Saídas
Lista de usuários que acessam o sistema.
Descrição das tarefas e fluxos de informação
A equipe de atendimento ao usuário da DTI, anualmente, consultará a solução de consulta de usuários credenciados e gerará uma lista, informando ao gestor da solução todos os usuários ativos no sistema sob sua gestão, com os respectivos perfis de acesso.
Descrição detalhada da atividade
-

Analisar criticamente a lista de usuários do sistema
Objetivo
Identificar autorizações de acesso(s) indevidos ao(s) sistema(s).
Início
Após receber a lista de usuários que acessam o sistema.
Entradas
Lista de usuários que acessam o sistema.
Saídas
Solicitação de revogação de acessos, se houver acessos indevidos.
Descrição das tarefas e fluxos de informação
Com base na lista de usuários ativos do sistema recebida da DTI, o Gestor da Solução irá avaliá-la em busca de identificar acessos indevidos, e, se houver, abrirá uma requisição na Central de Serviços, solicitando a revogação dos acessos pertinentes.
Descrição detalhada da atividade
-

NOTA: As atividades de registro de logs e rastreamento de acessos, para subsidiar auditoria e monitoramento, ainda não são tratadas neste subprocesso e serão implementadas gradativamente e mediante avaliação do esforço pela DTI.

[8] Portal de Serviços -> Sistemas -> Gestor de Solução de T.I.

ANEXO I - Indicadores de desempenho

Um indicador desempenho (Key Performance Indicator - KPI) é uma métrica utilizada para auxiliar no gerenciamento de um determinado processo.

A matriz a seguir documenta, em linhas gerais, os indicadores de desempenho a serem utilizados no subprocesso de Gestão do Credenciamento de Usuários de Sistemas:

Indicador	Descrição
Quantidade total de solicitações de acesso recebidas (concessão, alteração e revogação de acessos)	Indicação do volume total de solicitações de acesso recebidas dos usuários em um determinado período
Percentual de solicitações de acesso recebidas e não autorizadas	Indicação do % de solicitações de acesso recebidas dos usuários cuja autorização não foi provida, e por isso, o acesso não foi concedido, para um determinado período
Tempo médio de atendimento de solicitações de acesso	Indicação do tempo médio de atendimento das requisições de serviço referentes a solicitação de acesso tratadas em um determinado período
Índice geral de satisfação do usuário quanto ao atendimento de requisições de solicitações de acesso	Indicação do % de usuários satisfeitos com o atendimento de requisições de solicitações de acesso para um determinado período

OBS: Os relatórios poderão apresentar parametrização dos períodos da consulta, como dia, semana, mês ou ano, ou selecionar um período específico, bem como possibilitar a ordenação dos registros por diferentes critérios (data, tipo de solicitação, entre outros).

ANEXO II – Consultas operacionais

A seguir são descritas como podem ser realizadas as consultas operacionais às informações relacionadas à gestão do credenciamento de usuários de sistemas pela equipe de atendimento ao usuário:

OBJETIVO	FERRAMENTA	DETALHAMENTO
Consultar se a solução é um Sistema de Informação ou um Software Aplicativo	Ferramenta de gerenciamento de serviços de TI da CGU	Em [Catálogo de Serviços] → Categorização, informar [Categoria]: "Requisição de Serviço", [Subcategoria]: "Sistemas" ou "Aplicativos". No campo [Área] constará o nome da solução.
Consultar se a solicitação é atendida por meio da Central de Serviços	Portal de Serviços da CGU	No menu [Catálogo de Serviços], clicar em [Nova Requisição] → [Serviços de TI] → [Sistemas] → clicar no nome do sistema. Exibir detalhes do item de solicitação de acesso, pois nele será possível consultar se o item é informativo ou como solicitar o acesso.
Consultar se há requisitos adicionais de acesso ao sistema	Ferramenta de gerenciamento de serviços de TI da CGU	Em [Catálogo de Serviços] → Catálogo de Usuários, pesquisar pelo nome do Sistema. Clicar na linha referente ao [item] e verificar a aba [Seleções do Usuário]. Se não estiver preenchida, não há requisitos adicionais. Se estiver preenchida, apresentará os campos requeridos.
Consultar qual é o fluxo de aprovação do sistema	Ferramenta de gerenciamento de serviços de TI da CGU	Em [Catálogo de Serviços] → Categorização, informar [Categoria]: "Requisição de Serviço", [Subcategoria]: "Sistemas". Informar na [área] o nome do sistema e clicar em [pesquisar]. Selecionar o [tipo de problema] desejado e consultar a informação constante no campo [Fluxo].
Consultar qual é o grupo designado do sistema	Ferramenta de gerenciamento de serviços de TI da CGU	Em [Catálogo de Serviços] → Categorização, informar [Categoria]: "Requisição de Serviço", [Subcategoria]: "Sistemas". Informar na [área] o nome do sistema e clicar em [pesquisar]. Selecionar o [tipo de problema] desejado e consultar a informação constante no campo [Grupo Designado].
Consultar a lista de usuários por sistema ou a lista de sistemas que o usuário acessa	Ferramenta de consulta de usuários credenciados	http://office.com → aplicativo: Power BI → selecionar o aplicativo Credenciamento (também disponível no teams → Power BI → Credenciamento)
Consultar políticas, normas e orientações relacionados aos sistemas estruturantes da APF	Intranet da CGU	http://intra.cgu.gov.br -> Gestão Administrativa -> Tecnologia da Informação -> Sistemas -> Credenciamento de Usuários
Consultar a lista de sistemas abrangidos por este subprocesso	Intranet da CGU	http://intra.cgu.gov.br -> Gestão Administrativa -> Tecnologia da Informação -> Sistemas -> Credenciamento de Usuários

No momento de elaboração deste subprocesso, os produtos vigentes (em uso) correspondentes às ferramentas citadas neste documento, são:

- Base de conhecimento da CGU: DSPACE (https://basedeconhecimento.cgu.gov.br);
- Solução de consulta a usuários credenciados: Painel Power Bi Credenciamento (DTI/SE/CGU);
- Ferramenta de gerenciamento de serviços de TI da CGU: HP Service Manager (HPSM);
- Ferramenta de orquestração: HP Operations Orchestration software (HPOO);
- Ferramenta que processa eventos de pessoal: e-aud (https://eaud.cgu.gov.br);
- Portal de Serviços da CGU: https://servicos.cgu.gov.br

ANEXO III – Automação de descredenciamentos em alteração de acessos

A seguir, a lista de eventos de pessoal que são registrados no sistema de informação que processa os eventos de pessoal, e que geram automaticamente tickets para que se providencie o descredenciamento de usuários:

CATEGORIA DO EVENTO	**EVENTO**
Afastamento, licença ou penalidade	Afastamento para servir a outro órgão ou entidade
	Licença para afastamento do cônjuge ou companheiro
	Licença para tratar de interesses particulares
	Envolvimento em processo administrativo disciplinar (PAD)
Desligamento	Aposentadoria
	Demissão
	Exoneração
	Falecimento
	Posse em cargo inacumulável
	Retorno para órgão de origem
	Encerramento de atividades, contrato ou acordo com colaboradores