EMPRESA BRASILEIRA DE SERVIÇOS HOSPITALARES
SCS Quadra 9, Edifício Parque Cidade Corporate, Torre C, 1° ao 3° andares - Bairro Asa Sul
Brasília-DF, CEP 70308-200
(61) 3255-8900 - http://www.ebserh.gov.br

Norma Operacional - SEI nº 5/2022/SGTI/DTI-EBSERH

NORMA OPERACIONAL DE ACESSO E DISPONIBILIZAÇÃO DE DADOS DIGITAIS

Dispõe sobre a implementação do controle de acesso e disponibilização de dados armazenados em bancos de dados no âmbito da Administração Central e dos Hospitais Universitários Federais (HUFs) da Empresa Brasileira de Serviços Hospitalares - Ebserh.

A **DIRETORA DE TECNOLOGIA DA INFORMAÇÃO** da Empresa Brasileira de Serviços Hospitalares - Ebserh, no uso de suas atribuições institucionais, conferidas pelo artigo 103 do Regimento Interno da Administração Central da Ebserh, aprovado na 137ª Reunião Extraordinária do Conselho de Administração, realizada no dia 14 de junho de 2022, RESOLVE:

Divulgar a presente Norma Operacional que dispõe sobre a implementação do controle de acesso e disponibilização de dados no âmbito da Rede Ebserh.

CAPÍTULO I - DAS DISPOSIÇÕES INICIAIS

Seção I - Do Objeto e Âmbito de Aplicação

Art. 1º Esta norma operacional estabelece diretrizes para implementação do controle de acesso e disponibilização de dados armazenados em bancos de dados na Administração Central e nos Hospitais Universitários Federais (HUs) da Empresa Brasileira de Serviços Hospitalares (Ebserh), com o objetivo de garantir eficiência, segurança, privacidade e proteção dos dados digitais.

§ 1º O acesso e a disponibilização de dados se darão de forma controlada, com a devida permissão dos responsáveis, a fim de mitigar riscos, evitar a quebra de segurança da informação e preservar a proteção de dados pessoais.

§ 2º Esta norma não se aplica ao acesso a dados realizado por meio do uso dos sistemas de informação, como o Aplicativo de Gestão de Hospitais Universitários (AGHU), Sistema Eletrônico de Informações (SEI), Sistemas de Informações Gerenciais (SIG) e outros sistemas corporativos.

Art. 2º Esta norma aplica-se a todos os empregados, servidores, colaboradores, terceirizados, estagiários, estudantes, docentes, pesquisadores e consultores, corregedores e auditores, conveniados, credenciados, ou quaisquer outros indivíduos ou entidades que tenham acesso ou utilizem, direta ou indiretamente, os ativos de informação armazenados em bancos de dados da Rede Ebserh.

Seção II - Das Definições

Art. 3º Para os fins desta norma consideram-se os seguintes conceitos:

I - acesso a dados: consiste no ato de consultar ou processar dados digitais, em caráter temporário ou continuado, por usuários devidamente autorizados;

II - ativo de informação digital: são os ativos que suportam os meios de armazenamento, transmissão e processamento da informação, tais como: os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e os recursos humanos a eles associados;

III - área de TI: área responsável pelos recursos computacionais e sistemas de tecnologia da informação, sendo a Diretoria de Tecnologia da Informação (DTI) na Administração Central e o Setor de Tecnologia da Informação e Saúde Digital (SETISD) nos HUs da Ebserh;

IV - banco de dados: conjunto estruturado de dados, estabelecido em um ou em vários locais, em suporte eletrônico;

V - bloqueio de acesso: processo que tem por finalidade suspender temporariamente o acesso;

VI - concedente do acesso: Comitê de Concessão de Acesso e Disponibilização de Dados (CCAD);

VII - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder, bloquear ou revogar acessos ao uso de recursos computacionais;

VIII - contas de acesso: permissão, concedida por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso aos dados digitais;

IX - dado digital: informação preparada para ser processada, operada e transmitida por sistema de informação ou *software* e provisionada em banco de dados;

X - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

XI - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

XII - disponibilização de dados: consiste no compartilhamento ou transmissão de dados pela área de TI, em caráter pontual e por prazo definido, para usuários devidamente autorizados;

XIII - gestor da informação: agente público responsável pela administração das informações geridas nos processos de trabalho sob sua responsabilidade;

XIV - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;

XV - requerente do acesso: agente responsável por solicitar, para si ou para outrem, concessão, alteração, bloqueio e revogação de acesso ou disponibilização de dados armazenados em banco de dados da Ebserh;

XVI - revogação de acesso: processo que tem por finalidade suspender definitivamente o acesso ao dado digital, incluindo o cancelamento do código de identificação e do perfil de acesso;

XVII - tratamento de dados: toda operação realizada com dados digitais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

XVIII - usuário: pessoa física habilitada para acessar os dados digitais.

Seção III - Das Referências Legais e Normativas

Art. 4º A aplicação desta norma é orientada pela observância dos seguintes instrumentos legais e infralegais:

I - Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

II - Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

III - Norma complementar nº 07/IN01/DSIC/GSIPR, de 16 de julho de 2014, que estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

IV - Resolução do Conselho Federal de Medicina n.º 2.217, de 27 de setembro de 2018 - Código de Ética Médica;

V - Resolução 1.605/2000 do CFM, que dispõe sobre a revelação de conteúdo do prontuário ou ficha médica;

VI - Resolução do CNS 466/12 e normas complementares;

VII - Norma NBR ISO/IEC 27001/2013;

VIII - Norma NBR ISO/IEC 27002/2013;

IX - Política de Segurança da Informação da Ebserh;

X - Política de Proteção de Dados Pessoais da Ebserh;

XI - Política de Governança de Tecnologia da Informação da Ebserh; e

XII - Política de Gestão de Riscos e Controles Internos da Ebserh.

CAPÍTULO II - DO CONTROLE DE ACESSO E DISPONIBILIZAÇÃO DE DADOS DIGITAIS

Seção I - Do Escopo

Art. 5º O acesso e a disponibilização serão concedidos a usuário previamente autorizado pelo Comitê de Concessão de Acesso e Disponibilização de Dados (CCAD).

Art. 6º As concessões de acesso e disponibilização que trata esta norma aplicam-se às solicitações referentes aos dados armazenados em banco de dados de:

I - sistemas de informação ou *software* mantidos e geridos pela Administração Central da Ebserh;

II - sistemas de informação ou *software* mantidos e geridos pelas unidades hospitalares da Rede Ebserh; e

III - repositórios de arquivos e dados da Ebserh.

Seção II - Dos Papéis e Responsabilidades

Art. 7º A responsabilidade de avaliação do mérito do acesso aos dados ficará a critério da área negocial responsável pelo dado na instituição, não cabendo ao CCAD tal avaliação.

Art. 8º Podem ser habilitados como requerentes de acesso e disponibilização de dados da Rede Ebserh quaisquer empregados, servidores, colaboradores, terceirizados, estagiários, estudantes, docentes, pesquisadores, consultores, corregedores, auditores, conveniados ou credenciados que venham a utilizar, direta ou indiretamente, os ativos de informação armazenados em bancos de dados da Ebserh.

Parágrafo único. A análise e aprovação do acesso aos dados inerentes às atividades laborais dos empregados e colaboradores da Ebserh em suas unidades de lotação será de responsabilidade da chefia imediatamente superior.

A autorização para acesso e disponibilização.

Art. 9º São responsabilidades do Comitê de Concessão de Acesso e Disponibilização de Dados (CCAD):

I - aprovação da concessão, alteração, bloqueio ou revogação de acesso ou disponibilização de dados, considerando a finalidade da solicitação e as legislações aplicáveis;

II - definição dos critérios de temporalidade de contas de acesso dos requerentes;

III - monitoramento, publicação das alterações e busca de melhorias nos procedimentos de concessão de acessos; e

IV - gestão e controle dos acessos e disponibilização de dados, devendo manter registro formal e histórico dos acessos e disponibilizações concedidos, alterados, bloqueados ou revogados, bem como dos prazos e datas de expiração, dados estes abertos à consulta por parte da Auditoria;

Parágrafo único. Os Comitês de Concessão de Acesso e Disponibilização de Dados da Administração Central e das Unidades da Ebserh têm a incumbência de elaborar e propor seu Regimento Interno, seguindo orientações da Diretoria de Tecnologia da Informação, no prazo de até 90 (noventa) dias após a publicação desta Norma.

Art. 10. O CCAD é composto por, no mínimo, os seguintes membros:

I - na Administração Central: um representante da Vice-Presidência (VP); um representante da Diretoria de Ensino, Pesquisa e Atenção à Saúde (DEPAS); um representante da Diretoria de Gestão de Pessoas (DGP); um representante da Diretoria de Administração e Infraestrutura (DAI); e um representante da Diretoria de Tecnologia da Informação (DTI), que exercerá a coordenação técnica do CCAD; e

II - nos HUs: um representante da Superintendência (SUP); um representante da Gerência de Atenção à Saúde (GAS); um representante da Gerência de Ensino e Pesquisa (GEP); um representante da Gerência Administrativa (GAD); e um representante do Setor de Tecnologia da Informação e Saúde Digital (SETISD), que exercerá a coordenação técnica do CCAD.

Parágrafo Único. Poderão ser convidados a participar do CCAD representantes de outras áreas da Ebserh.

Art. 11. As áreas de TI deverão executar, uma vez aprovadas pelo CCAD, as atividades de concessão, alteração, bloqueio ou revogação de acesso a dados da Rede Ebserh.

§ 1º As áreas de TI são responsáveis pela manutenção, sustentação e guarda dos dados armazenados nos bancos de dados sob sua responsabilidade.

§ 2º Em casos excepcionais, como demandas judiciais e de auditoria interna, a disponibilização de dados poderá ser realizada diretamente pela área de TI, com comunicação posterior à CCDA.

Art. 12. O monitoramento dos acessos concedidos será realizado pela Diretoria de Tecnologia da Informação, na Administração Central, e pelo Setor de Tecnologia da Informação e Saúde Digital, nos hospitais.

Parágrafo Único. Em caso de acessos distintos dos acessos permitidos, a área de TI encaminhará o caso à CCAD para análise e definição das providências cabíveis.

Art. 13. A matriz de papéis e responsabilidades das partes do processo deve observar a seguinte estrutura:

Atividades	Requerente	CCAD Concedente	Área de TI
Solicitar concessão, alteração, bloqueio ou revogação de acesso a dados.	X		
Receber as demandas de concessão ou alteração de acesso a dados.		X	
Analisar as solicitações de concessão ou alteração de acesso a dados, se adequadas às orientações desta norma.		X	
Solicitar o bloqueio e revogação de acesso a dados quando necessário, conforme orientações desta norma.		X	
Registrar ciência na aprovação ou não do acesso aos dados.	X		
Realizar a gestão e controle dos acessos aos dados.		X	
Receber as aprovações do CCAD e conceder acesso aos dados, conforme orientações do Comitê.			X
Registrar ciência na concessão ou não de acesso aos dados.	X		
Monitorar os acessos e disponibilização de dados.			X

Tabela 1 – Matriz de Papéis e Responsabilidades

Seção III - Da Solicitação de Acesso ou Disponibilização

Art. 14. A solicitação de acesso e disponibilização de dados está condicionada ao preenchimento e assinatura de Termo de Responsabilidade para Acesso a Dados pelo requerente, conforme modelo constante no Anexo I desta norma.

I - o requerente deverá abrir processo SEI do tipo "Gestão da Informação: Gestão da Segurança da Informação", inserir, preencher e assinar o documento SEI: "Termo de Responsabilidade para Acesso a Dados", que compreende minimamente os seguintes elementos:

a) identificação do requerente do acesso;

b) identificação da informação a ser acessada e do tipo do dado;

c) justificativa para a concessão do acesso e disponibilização dos dados, apresentando a necessidade e a finalidade de tal acesso, demonstrando sua boa-fé, sempre observando os princípios da LGPD;

d) período de acesso (data estimada de início e encerramento);

e) assinatura do requerente;

f) declaração de compromisso quanto à proteção e segurança de possíveis informações confidenciais e outros, conforme Anexo I desta norma; e

g) demais informações necessárias à clareza da solicitação.

II - caso o requerente não possua acesso ao SEI, o mesmo deverá elaborar requerimento conforme modelo constante no Anexo I desta norma e entregá-lo na área de protocolo, destinada à recepção de documentos externos ou, na inexistência deste, diretamente ao CCAD;

III - caso o requerente seja empregado da Ebserh, o termo também deverá ser assinado pela chefia imediata, para ciência da solicitação;

IV - o termo deve ser encaminhado para o CCAD do respectivo HU ou para o CCAD da Administração Central quando se referir a dados de mais de um hospital da Rede Ebserh.

Parágrafo Único. Em caso de projeto de pesquisa, será aceito o termo de autorização da DEPAS, na Administração Central, e da GEP, nos hospitais, desde que atendido os requisitos acima.

Seção IV - Da Aprovação da Solicitação de Acesso ou Disponibilização

Art. 15. A aprovação do acesso e disponibilização de dados será de responsabilidade do CCAD do respectivo HU, ou da Administração Central quando se referir a mais de um hospital da Rede Ebserh.

Parágrafo Único. No caso de solicitações decorrentes de projetos de pesquisa, estas devem estar inseridas no Sistema Rede Pesquisa e acompanhadas da aprovação do Gerente de Ensino e Pesquisa do respectivo hospital, ou do Diretor de Ensino, Pesquisa e Atenção à Saúde, quando se referir a dados de mais de um hospital da Rede Ebserh.

Art. 16. O CCAD analisará o Termo de Responsabilidade para Acesso a Dados, encaminhado pelo requerente, observando a pertinência das informações, prazos, tipos de acessos, finalidade e justificativas apresentadas, de acordo com as orientações desta norma.

§1º O CCAD convocará o gestor da informação, responsável pelo ativo de informação digital, para deliberar sobre a aprovação dos acessos.

§2º Caso identificada incorreção no preenchimento do termo ou justificativas insuficientemente motivadas, o processo será devolvido para correção, ajustes ou complemento pelo requerente.

Art. 17. Em caso de aprovação, o CCAD encaminhará despacho de aprovação para a área de TI, conforme modelo constante no Anexo II desta norma, no qual deverão ser informados os dados, documentos ou arquivos, cujos acessos serão concedidos, bem como o período e formato adequado do acesso:

I - concessão de acesso dos dados ao requerente;

II - disponibilização dos dados ao requerente, devendo ser informado quais dados necessitarão de tratamento, anonimização ou pseudonimização.

Art. 18. Em caso de reprovação, o CCAD devolverá o processo ao requerente, informando as razões da recusa ao acesso solicitado.

Art. 19. As solicitações de prorrogação de prazo, alterações, bloqueios ou revogações de acesso ou disponibilização também serão de responsabilidade do CCAD, devendo ser encaminhadas à área de TI, para as providências técnicas necessárias.

Seção V - Da Concessão de Acesso e Disponibilização dos Dados pela Área de TI

Art. 20. Após aprovação da concessão do acesso ou disponibilização de dados pelo CCAD, a área de TI dará prosseguimento técnico à concessão.

Parágrafo Único. Além da concessão de acesso e disponibilização dos dados, a área de TI também deve atender as solicitações de alteração, bloqueio ou revogação de acesso recebidas do CCAD.

Seção VI - Demais Diretrizes para Implementação do Controle de Acesso a Dados

Art. 21. São ainda diretrizes para implementação de controles de acesso a serem observadas pela área de TI da Ebserh:

I - disponibilizar dados ou conceder acesso aos ambientes de rede onde estão armazenados os ativos de informação, após aprovação do CCAD;

II - revogar acesso dos requerentes aos ambientes de rede onde estão armazenados os ativos de informação quando do término do período de acesso;

III - registrar os acessos aos ambientes de rede de forma a permitir a rastreabilidade e a identificação do requerente;

IV - utilizar mecanismos automáticos de segurança para inibir que equipamentos externos conectem-se aos ambientes de Ebserh;

V - manter, nos ambientes de rede, mecanismos que permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados;

VI - utilizar canal seguro para a concessão de acesso remoto;

VII - gravar o acesso remoto aos ambientes de rede em logs, para posterior auditoria, contendo informações específicas que facilitem o rastreamento da ação executada;

VIII - disponibilizar ao requerente, sempre que possível, somente uma única conta institucional de acesso, pessoal e intransferível;

IX - conceder conta de acesso no perfil de administrador somente para requerentes cadastrados para execução de tarefas específicas da administração de ativos de informação;

X - utilizar, sempre que possível, ferramentas de proteção contra acesso não autorizado aos ativos de informação, que favoreçam, preferencialmente, a administração de forma centralizada;

XI - registrar eventos relevantes, previamente definidos, para a segurança e rastreamento de acesso às informações;

XII - nos casos de acesso ou disponibilização de dados, deve-se considerar, sempre que possível, sua anonimização ou pseudonimização;

XIII - no caso de dados criptografados, a senha não poderá ser enviada no mesmo meio onde serão depositadas as informações, visando maior segurança em caso de perda, furto, roubo ou cópia mal-intencionada;

Art. 22. A Administração Central e os HU, em suas áreas de competência, deverão observar o fluxo do processo para concessão de acessos e disponibilização de dados constante no Anexo III desta norma.

Art. 23. Em caso de utilização de mídia, o material a ser utilizado será de responsabilidade do requerente da informação.

Parágrafo Único. É de responsabilidade do requerente da informação garantir a confidencialidade e o sigilo dos dados institucionais disponibilizados em mídia, bem como de sua adequada remoção, quando aplicável.

Art. 24. A disponibilização de dados para projetos de inovação tecnológica devem, além do contemplado nessa norma, prever acordo de propriedade intelectual.

Parágrafo Único. Cláusulas de propriedade intelectual deverão ser elaboradas em instrumento jurídico próprio tratados com a Diretoria de Ensino, Pesquisa e Atenção à Saúde.

CAPÍTULO III - DAS DISPOSIÇÕES FINAIS

Art. 25. Esta norma se aplica a todos os acessos e disponibilização de dados digitais da Ebserh, devendo ser revogados e/ou adequados os que estiverem em desconformidade com esta norma, no prazo de até 120 (cento e vinte) dias.

Art. 26. Havendo indícios de descumprimento da presente norma, caberá ao CCAD encaminhar processo à autoridade competente para avaliação dos fatos e considerações, sujeitando os agentes responsáveis às sanções administrativas cabíveis, após ser oportunizado o contraditório e a ampla defesa, nos termos da normativa específica.

Art. 27. O não cumprimento desta norma poderá resultar em apuração de responsabilidade.

Art. 28. Todo usuário tem o dever de reportar, de imediato e por escrito à área de TI, qualquer incidente de segurança identificado, tais como acesso não autorizado, acidental ou ilícito, que resulte na destruição, perda, alteração, vazamento de dados ou ainda qualquer infração a esta norma, à LGPD e demais elementos da Política de Segurança da Informação.

Art. 29. Os casos omissos ou situações não previstas nesta norma serão decididos pelo CCAD.

Art. 30. Esta norma entra em vigor na data de sua publicação.

(assinado eletronicamente)
SIMONE HENRIQUETA COSSETIN SCHOLZE
Diretora de Tecnologia da Informação

ANEXO I
MODELO DE TERMO DE RESPONSABILIDADE PARA ACESSO A DADOS

DADOS DO REQUERENTE DO ACESSO OU DISPONIBILIZAÇÃO DOS DADOS

Nome:

CPF:

Cargo:

Lotação:

Telefone:

E-mail:

INFORMAÇÃO A SER ACESSADA:

Quais dados deseja ter acesso: *[informar quais arquivos, documentos ou dados de sistemas que será necessário ter acesso]*

Ambiente de Acesso: *[desenvolvimento, teste, treinamento, homologação, backup, consulta e/ou produção]*

O acesso solicitado contém que tipo de dados: *[informar se os arquivos a serem acessados possuem dados do tipo público, pessoal ou pessoal e sensível]*

JUSTIFICATIVA PARA A CONCESSÃO DO ACESSO E DISPONIBILIZAÇÃO DOS DADOS

Inserir justificativa: *[A justificativa deverá ser motivada e elaborada de forma clara, precisa e suficiente, sendo vedadas justificativas genéricas e que sejam incapazes de demonstrar, de forma cabal, a necessidade do acesso aos dados]*

PERÍODO DE ACESSO

Por qual período será necessário o acesso: *[especificar o período necessário do acesso, exemplo: 30 dias; 90 dias; 180 dias; 1 ano; indeterminado; ou informar data de início e término]*

Obs.: Demais informações, documentos ou anexos que se fizerem necessários à clareza deste Termo de Responsabilidade para Acesso a Dados deverão ser inseridos no processo.

Ao assinar este Termo, declaro-me ciente de que:

a) os dados acessados serão utilizados apenas para os propósitos expressamente informados neste Termo e não para fins diversos, sob pena de responsabilização administrativa, civil e penal;

b) não devo reproduzir, divulgar, compartilhar, revelar, publicar ou realizar cópias, em meio físico ou eletrônico, das informações acessadas, sem a devida autorização do Colegiado Executivo do respectivo Hospital Universitário Federal ou da Diretoria Executiva da Ebserh, quando se tratar de mais de um hospital;

c) devo tomar todas as medidas necessárias à proteção dos dados, bem como me comprometo a manter o sigilo e a confidencialidade dos dados, em especial dados pessoais e dados pessoais sensíveis, sob pena de responsabilidade administrativa, civil e penal;

d) responsabilizo-me pela proteção e segurança de possíveis informações confidenciais acessadas nos dados disponibilizado pela Ebserh, tais como dados pessoais e pessoais sensíveis, com vistas a observar e atender as regras da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais).

d.1) entende-se como dados pessoais: nome, data de nascimento e/ou idade, sexo, nacionalidade, estado civil, número e cópia dos documentos de identificação profissional, CPF, RG, RNE, PIS, habilitações, contrato porventura celebrado, função/cargo, matrícula, remuneração, local de trabalho, fotografia, endereço de residência, e-mail, telefones, dados de familiares e/ou dependentes e outros.

d.2) entende-se como dados pessoais sensíveis: biometria, raça/cor, filiação sindical, dados relacionados à saúde ou à vida sexual, convicção religiosa e outros.

e) a conta de acesso é pessoal e intransferível, sendo obrigatória a manutenção sigilosa da mesma, não podendo, em hipótese alguma, ser compartilhada, ainda que em caráter emergencial ou por necessidade de serviço.

f) devo comunicar, de imediato e por escrito, ao Comitê de Concessão de Acesso e Disponibilização de Dados (CCAD), bem como à área de TI, qualquer incidente de segurança identificado, bem como qualquer evento adverso confirmado, tais como acesso não autorizado, acidental ou ilícito, que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma inadequada ou ilícita de tratamento de dados.

g) comprometo-me a observar e cumprir:

g.1) a Norma Operacional de Acesso e Disponibilização de Dados Digitais da Ebserh;

g.2) a Política de Proteção de Dados Pessoais da Ebserh;

g.3) a Política de Segurança da Informação da Ebserh;

g.4) a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), bem como os demais normativos e orientações referentes ao sigilo e segurança de dados, respondendo administrativa e judicialmente por eventuais danos causados à Ebserh ou a outrem.

(assinado eletronicamente)
Nome do Requerente
Cargo

No caso de empregado Ebserh, colher assinado pela chefia imediata, para demonstração da ciência.

ANEXO II
MODELO DE DESPACHO DE AUTORIZAÇÃO PARA CONCESSÃO DE ACESSO OU DISPONIBILIZAÇÃO DOS DADOS

À *[Área de TI do respectivo HU ou da Administração Central]*

Após análise do Termo de Responsabilidade para Acesso a Dados (xxxxxxx) e observando-se a pertinência das informações, finalidade, justificativa, prazos e tipos de acessos, de acordo com as orientações da Norma de Acesso e Disponibilização de Dados, a LGPD e demais legislações vigentes, este Comitê de Concessão de Acesso e Disponibilização de Dados **AUTORIZA** a concessão de acesso ao requerente *[informar nome completo e CPF do requente do acesso],* aos seguintes dados da *[Unidade da Rede Ebserh]*:

- *Informar para quais arquivos, documentos ou dados de sistemas que deverão ser concedido o acesso;*
- O formato do acesso: *por liberação de acesso ou por meio de envio de arquivos ao requerente ou outro, devendo ser informados quais dados necessitarão de tratamento, anonimização ou pseudonimização;* e
- *O período total do acesso.*

A conta de acesso é intransferível, sendo obrigatória a manutenção sigilosa da mesma, não podendo, em hipótese alguma, ser compartilhada, devendo ser utilizada no estrito cumprimento das funcionalidades concedidas e devidamente revogadas após o término de sua validade.

(assinado eletronicamente)	*(assinado eletronicamente)*	*(assinado eletronicamente)*
Nome Completo	Nome Completo	Nome Completo
Membro do CCAD	Membro do CCAD	Membro do CCAD

ANEXO III

FLUXO DO PROCESSO DE GESTÃO E CONTROLE DOS ACESSOS

1. A Administração Central e os HU, em suas áreas de competência, deverão observar o seguinte fluxo para concessão de acessos ou disponibilização de dados:

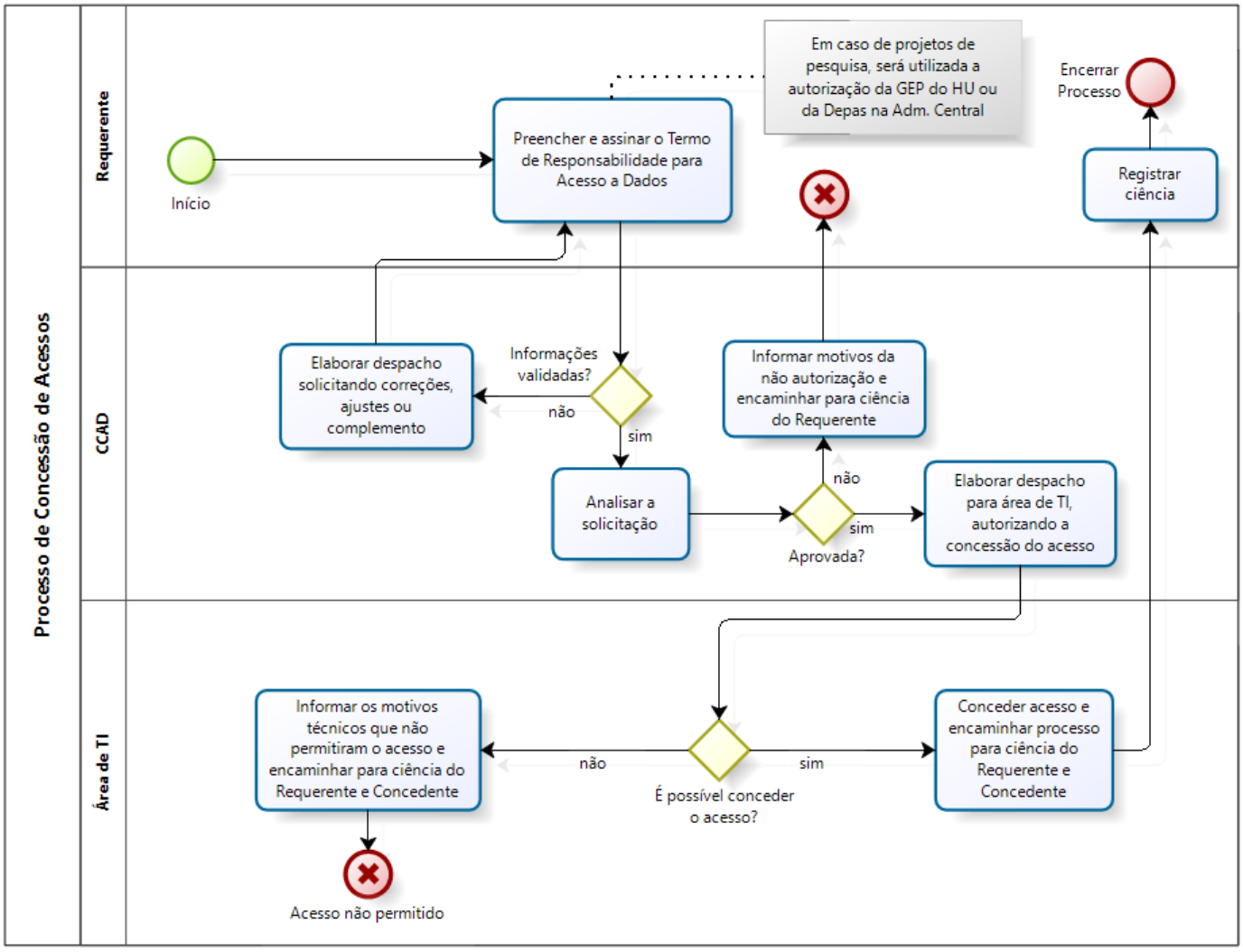

Figura 01 - Fluxo do Processo de Concessão de Acessos

1.1. O requerente, ao obter acesso aos dados, deverá zelar pela confidencialidade de sua senha e segurança dos dados acessados, atendendo a todas as regras estabelecidas nesta norma, LGPD e demais legislações vigentes acerca do tema.

2. Quando da necessidade de bloqueio ou revogação do acesso, a Administração Central e os HUs, em suas áreas de competência, deverão observar o seguinte fluxo:

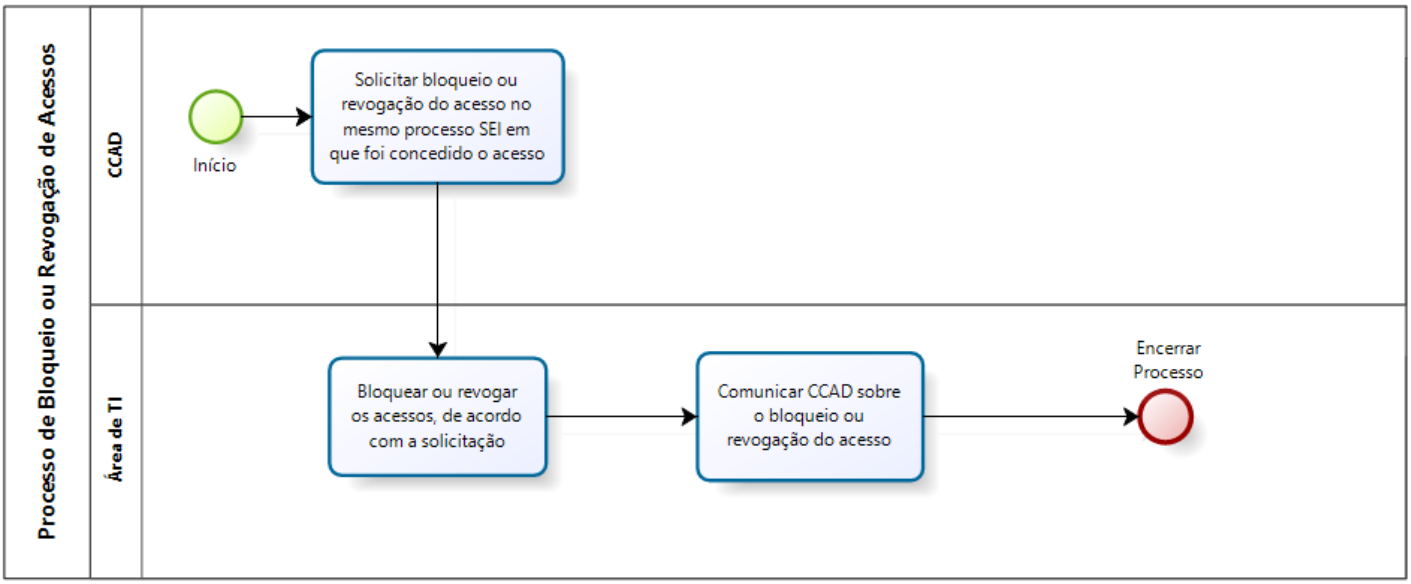

Figura 02 - Fluxo do Processo de Bloqueio ou Revogação de Acessos

2.1. Os acessos concedidos podem ser boqueados ou revogados a qualquer tempo, por decisão do CCAD, a pedido da Coordenadoria de Consultoria Jurídica, do Comitê de Segurança da Informação, da Auditoria, do Colegiado Executivo ou da Diretoria Executiva da Ebserh.

Documento assinado eletronicamente por **Simone Henriqueta Cossetin Scholze**, **Diretor(a)**, em 19/12/2022, às 16:00, conforme horário oficial de Brasília, com fundamento no art. 6º, caput, do Decreto nº 8.539, de 8 de outubro de 2015.

Referência: Processo nº 23477.011135/2021-32 SEI nº 25947184