Governança

POL – 0008_Política de Controle de Acesso

Histórico de Versões

Data	Versão	Descrição	Autor
18/01/2024	1.0	POL – 0008_Política de Controle de Acesso	Angélica Ferreira
12/03/2024	2.0	POL – 0008_Política de Controle de Acesso	Angélica Ferreira

Aviso Preliminar

O presente documento visa a auxiliar no entendimento da Política de Controle de Acesso, em atendimento ao previsto no art. 46 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que determina que a Liberty TI, ao prestar diversos serviços que tratam dados pessoais à sociedade, deve adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito dos dados que estão sob sua custódia. Adicionalmente, a Elaboração de uma Política de Controle de Acesso visa a atender, além da LGPD, a outros normativos vigentes sobre o tema de privacidade e segurança da informação.

Este documento é de autoria exclusiva da Liberty Health Tech e tem como referência fundamental o Guia do Framework de Privacidade e Segurança da Informação baseado em diversas publicações e documentos técnicos já existentes que são utilizados amplamente por profissionais da área de privacidade e segurança da informação. Destacam-se as publicações do Center for Internet Security (CIS), da International Organization for Standardization (ISO) e do National Institute of Standards and Technology (NIST). Com o objetivo de facilitar a difusão de conhecimentos sobre privacidade e segurança da informação, tais referências, quando escritas em línguas estrangeiras, foram traduzidas para o português pela equipe técnica da Diretoria de Privacidade e Segurança da Informação da Liberty Health Tech.

Nesse cenário, a Liberty Health Tech enfatiza que:

a) não representa, tampouco se manifesta em nome do CIS, da ISO e do NIST e vice-versa;
b) não se manifesta em nome de autoridades de privacidade e segurança da informação;
c) não é coautora das publicações internacionais abordadas;
d) não assume nenhuma responsabilidade administrativa, técnica ou jurídica por usos ou interpretações inadequadas, fragmentados ou parciais do presente Documento; e
e) caso o leitor deseje se certificar de que atende integralmente os requisitos das publicações das instituições mencionadas, deverá consultar diretamente as fontes oficiais de informação ofertadas por elas, que foram listadas na seção “Referência Legal e de Boas Práticas” deste documento.

Este Documento será atualizado frequentemente, de acordo com as novas diretrizes determinadas pelas autoridades em privacidade e segurança da informação ou segundo eventuais alterações que ocorram nos normativos vigentes relacionados a privacidade e segurança da informação e outras referências utilizadas neste documento.

Introdução

Este Documento tem por finalidade apresentar orientações com o intuito de auxiliar os órgãos e Liberty Health Tech a elaborar sua Política de Controle de Acesso no âmbito institucional.

Nesse contexto, as organizações, com infraestrutura própria ou contratada de terceiros, coletam, recebem, acessam, processam, modificam, produzem, extraem, validam, armazenam, distribuem e transmitem informações confidenciais e públicas para apoiar a entrega de produtos e serviços essenciais (por exemplo, fornecimento de serviços financeiros; fornecimento de serviços de emissões guias, certificados e carteiras; processamento de autorizações de segurança ou dados de saúde; fornecimento de serviços em nuvem; desenvolvendo comunicações via cabo, wireless e/ou satélites; sistemas militares de defesa). As informações federais são frequentemente fornecidas ou compartilhadas, obedecidos os requisitos legais.

A proteção dessas informações pela Liberty Health Tech enquanto agente de tratamento está designada no **art. 46 da Lei Geral de Proteção de Dados**, sancionada em 14 de agosto de 2018:

> *"Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."*

Importante ressaltar que adoção deste documento não dispensa o órgão de considerar as diretrizes gerais estabelecidas para implementação da Política de Segurança da Informação, conforme prevê o art.12, Inciso IV da Instrução Normativa Nº 01/GSI/PR, bem como os Capítulos III e IV da Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021, a qual dispõe sobre os processos relacionados à gestão de Segurança da Informação na Liberty Health Tech.

Propósito

O objetivo da Política de Controle de Acesso é estabelecer controles de identificação, autenticação e autorização para salvaguardar as informações da Liberty Health Tech, estejam elas em qualquer meio, seja digital ou físico, a fim de evitar a quebra da segurança da informação e quaisquer acessos não autorizados que implique em risco de destruição, alteração, perda, roubo ou divulgação indevida.

Sem controles de autorização, identificação e autenticação, existe o risco potencial de que os sistemas de informação possam ser acessados ilicitamente e que a segurança desses sistemas de informação seja comprometida.

Considera-se, portanto, que as credenciais: crachá de identificação funcional e logins de acesso dos sistemas de informações, acesso biométrico facial e digital, são pessoais e intransferíveis e são o único método legítimo pelo qual o direito de acesso físico e/ou lógico podem ser exercidos.

Os controles de autorização, identificação e autenticação garantem que apenas usuários autorizados tenham acesso físico ou façam uso dos sistemas de informação da Liberty Health Tech.

Escopo

Esta Política se aplica a todas as informações, cuja Liberty Health Tech seja o agente de tratamento, ao meio utilizado para este tratamento, seja digital ou físico, e as dependências físicas desta organização, bem como a qualquer pessoa que circule nas dependências ou que interaja exercendo controle administrativo, técnico ou operacional, mesmo que eventual, desses meios de tratamento.

Especificamente, inclui:

- Todos os funcionários, sejam profissionais efetivos ou temporários, da Liberty Health Tech.
- Todos os funcionários de clientes e parceiros que acessam fisicamente as dependências ou que acessam a rede e sistemas e softwares de informação da Liberty Health Tech.

Termos e Definições

ACESSO - ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

CONTA DE SERVIÇO - conta de acesso à rede corporativa de computadores, necessária a um procedimento automático (aplicação, script, entre outros) sem qualquer intervenção humana no seu uso;

CONTROLE DE ACESSO - conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Geralmente, requer procedimentos de autenticação;

MFA - sigla de autenticação de multifatores (multifactor authentication);

Referência legal e de boas práticas

Orientação	Secção
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II art. 50

Declarações da Política

CAPÍTULO I

ACESSO LÓGICO

Art. 1º O acesso lógico aos recursos da Rede será realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pela Área de Infraestrutura, baseado nas responsabilidades e tarefas de cada usuário.

I. Terão direito a acesso lógico aos recursos da Rede os usuários de recursos de tecnologia da informação.

II. Para fins desta Resolução, consideram-se usuários de recursos de tecnologia da informação colaboradores, prestadores de serviço assim como funcionários de empresas prestadoras de serviços, estagiários e demais usuários temporários em atividade na Liberty Health Tech, ou profissionais que atuam utilizando o ambiente de nossos clientes.

III. O acesso remoto será realizado por meio de VPN – Rede Virtual Privada, após as devidas autorizações.

Art. 2º A Área de Infraestrutura, estabelecerá e manterá um inventário de todas as contas gerenciadas, este deve incluir contas de usuário, administrativas, testes e serviço. Em caso de contas de serviço, o inventário deve conter no mínimo informações de:

a. Departamento proprietário.
b. Data de criação/última autorização de renovação de acesso;
c. A Área de Infraestrutura, será a responsável por validar todas as contas ativas, periodicamente.

Art. 3º A Área de Infraestrutura atua com a centralização da gestão de contas por meio de serviço de diretório e/ou identidade denominado como AD (Active Directory).

Art. 4º A Área de Infraestrutura estabelecerá e manterá um inventário dos sistemas de autenticação e autorização da organização, tal inventário deve ser revisado periodicamente.

Art. 5º A Área de Infraestrutura definirá e manterá o controle de acesso dos usuários baseado em necessidade dos indivíduos, conforme as suas atribuições profissionais.

I. Deve ser elaborada a documentação dos direitos dos acessos para cada função dentro da organização.
II. A Área de Infraestrutura realizará análises de controle de acesso aos ativos institucionais para validar se todos os privilégios estão autorizados para a execução de atividades de cada função, este processo deve ser repetido de forma periódica ou quando novas funções e ativos de informação forem inseridos na organização.

CAPÍTULO II

CONTA DE ACESSO LÓGICO E SENHA

Art. 8º Para utilização das estações de trabalho da Liberty Health Tech, será obrigatório o uso de uma única identificação (*login*) e de senha de acesso, fornecidos pela Área de Infraestrutura, mediante solicitação formal do responsável pela Gestão ou RH.

I. Será necessário o envio de solicitação para criação de usuário, submetendo a solicitação para a Área de Infraestrutura, através de e-mail infra@libertyti.com.br, contendo as seguintes informações: Nome completo, Cargo, CPF do usuário, além do Nome do superior direto e/ou RH que acompanhará as funções do usuário a ser registrado. A resposta da solicitação de acesso será encaminhada a todos os envolvidos na solicitação inicial pelo mesmo meio em que foi submetida.

II. Os privilégios de acesso dos usuários à Rede devem ser definidos pelo requisitante, ao qual o usuário está vinculado, limitando-se a atividades estritamente necessárias à realização de suas tarefas.

III. Na necessidade de utilização de perfil diferente do disponibilizado, o requisitante, ao qual o usuário está vinculado, deverá encaminhar solicitação para a Área de Infraestrutura que a examinará, podendo negá-la nos casos em que a entender desnecessária.

Art. 9º O *login* e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados pelo Área de Infraestrutura quando constatada qualquer irregularidade.

Parágrafo único. Para retomar o acesso à rede, deverá ser formalizada nova requisição pelo responsável/RH.

Art. 10º O padrão adotado para o formato da conta de acesso do usuário é a sequência primeiro nome + ponto + último nome do usuário, como por exemplo, João.Silva.

Parágrafo único. Nos casos de já existência de conta de acesso para outro usuário, a Área de Infraestrutura e Segurança realizará outra combinação utilizando o nome completo do usuário para o qual a conta está sendo criada.

Art. 11º O padrão adotado para o formato da senha é o definido pelo Área de Infraestrutura, que considera o tamanho mínimo de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores.

I. A formação da senha da identificação (*login*) de acesso à Rede, deve seguir as regras de:

a) Possuir tamanho mínimo de oito caracteres, sendo obrigatório o uso de letras e números, para contas que utilizam MFA e 14 caracteres para contas que não utilizam MFA;
b) Recomenda-se a utilização de letras maiúsculas, minúsculas e caracteres especiais ($, %, &, ...);
c) Não ser formada por sequência numérica (123...), alfabética (abc...), nomes próprios, palavras de fácil dedução, datas, placa de carro, número de telefone, a própria conta de acesso, apelidos ou abreviações;
d) Não utilizar termos óbvios, tais como: Brasil, senha, usuário, *password* ou *system;*

II. A Área de Infraestrutura fornecerá uma senha temporária para cada conta de acesso criada no momento da liberação dessa conta e a mesma deverá ser alterada pelo usuário quando do primeiro acesso à Rede.

Parágrafo único. Caso não efetue a troca no prazo estabelecido, será bloqueado seu acesso à Rede até que a nova senha seja configurada.

CAPÍTULO III

CANCELAMENTO DA CONTA DE ACESSO

Art. 13º A conta de acesso será cancelada nos seguintes casos:

I. Solicitação do responsável imediato do usuário com a devida justificativa;

II. Quando da suspeita de mau uso dos serviços disponibilizados pelo Liberty Health Tech, ou descumprimento da Política de Segurança da Informação – e normas correlatas em vigência.

Art. 14º O desbloqueio da conta de acesso à Rede será realizado apenas após solicitação formal do responsável imediato do usuário a Segurança da Informação.

Art. 16º A conta de acesso será cancelada por encerramento de vínculo na prestação de serviços entre os profissionais com a Liberty Health Tech.

CAPÍTULO IV

MOVIMENTAÇÃO INTERNA

Art. 19º Quando houver mudança do usuário para outro setor ou o usuário ocupar uma nova função, os direitos de acesso à Rede devem ser revogados.

I. O responsável imediato ou o Área de RH deve realizar a solicitação de novos acessos a Área de Infraestrutura, de acordo com novo setor / função do usuário.

II. Os direitos de acesso antigos devem ser imediatamente cancelados através de solicitação do responsável imediato.

CAPÍTULO V

CONTA DE ACESSO BIOMÉTRICO

Art. 20º A conta de acesso biométrico, quando implementada, deve ser vinculada a uma conta de acesso lógico e ambas devem ser utilizadas para se obter um acesso, a fim de atender os conceitos da autenticação de multifatores.

Parágrafo único. A Liberty Health Tech deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

CAPÍTULO VI

ADMINISTRADORES

Art. 21º A utilização de identificação (*login*) com acesso no perfil de administrador é permitida somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

I. Somente os técnicos autorizados pela área de Infraestrutura, devidamente identificados e habilitados, terão senha com privilégio de administrador nos equipamentos locais e na rede.

II. Na necessidade de utilização de *login* com privilégio de administrador do equipamento local, o usuário deverá encaminhar solicitação para a Área de Infraestrutura, que poderá negar os casos em que entender desnecessária a utilização.

III. Se concedida a permissão ao usuário como administrador local na estação de trabalho, esse será responsável por manter a integridade da máquina.

IV. Caso constatada a irregularidade, o usuário perderá o acesso como administrador, não mais podendo requerer outra permissão.

CAPÍTULO VII

RESPONSABILIDADES

Art. 22º É de responsabilidade do responsável imediato do usuário comunicar formalmente o RH e o Área de Infraestrutura, o desligamento ou saída do usuário da Liberty Health Tech, para que as permissões de acessos sejam canceladas.

Art. 23º Caberá ao responsável da área em que haverá o desligamento a comunicação imediata ao RH da Liberty Health Tech para que seja efetuado o cancelamento definitivo da permissão de acesso aos recursos.

Art. 24º É responsabilidade do RH da Liberty Health Tech a comunicação imediata a Área de Infraestrutura da Informação sobre desligamentos e revogação definitiva da permissão de acesso aos recursos.

I. Os serviços serão filtrados por programas de *antivírus*, e, caso violem alguma regra de configuração, serão notificados para devidas ações necessárias.

II. Apenas a equipe de Infraestrutura, ou outras autorizadas pela área, terá acesso ao conteúdo das informações armazenadas nos servidores da Liberty Health Tech.

Art. 25º O usuário é responsável por todos os acessos realizados através de sua conta de acesso, e por possíveis danos causados à Rede e a recursos de tecnologia custodiados ou de propriedade da Liberty Health Tech.

I. O usuário é responsável pela integridade e utilização de sua estação de trabalho, devendo, no caso de sua ausência temporária do local onde se encontra o equipamento, bloqueá-lo ou desconectar-se da estação, para coibir acessos indevidos.

II. A utilização simultânea da conta de acesso à Rede em mais de uma estação de trabalho, notebook ou dispositivos móveis devem ser evitadas, sendo responsabilidade do usuário titular da conta de acesso os riscos que a utilização paralela implica.

III. O usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha.

Art. 26º O usuário deve informar a um responsável direto, qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.

Art. 27º É dever de o usuário zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para a Instituição, a saber:

I. Não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros, e outras formas;

II. Evitar sobrecarga de redes, de dispositivos de armazenamento de dados ou de outros, para não gerar indisponibilidade de informações internas e externas;

III. Interromper a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completarem suas atividades ou quando se ausentarem do local de trabalho por qualquer motivo;

IV. Não se conectar a sistemas e não buscar acesso a informações para as quais não lhe tenham sido dadas senhas e/ou autorização de acesso;

V. Não divulgar a terceiros ou a outros usuários dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas;

VI. Utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e medidas preventivas estabelecidas;

VII. Não divulgar suas senhas e nem permitir que terceiros tomem conhecimento delas, reconhecendo-as como pessoais e intransferíveis;

VIII. Assinar o Termo de Responsabilidade (Documento – Anexo I) quanto a utilização da respectiva conta de acesso.

CAPÍTULO VIII

DISPOSIÇÕES GERAIS

Art. 29º Os incidentes que afetem a Segurança das Informações, assim como o descumprimento da Política de Segurança da Informação e Normas de Segurança devem ser obrigatoriamente comunicados pelos usuários a Área de Infraestrutura / setor de segurança.

Art. 30º Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, o Área de Infraestrutura e Segurança fará a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.

I. Nos casos em que o autor da quebra de segurança for um usuário, o Área de Infraestrutura comunicará os resultados ao responsável direto do mesmo para adoção de medidas cabíveis.

II. Ações que violem a Política de Segurança da Informação ou que quebrem os controles de Segurança da Informação serão passíveis de sansões civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente.

III. A resolução de casos de violação/transgressões omissos nas legislações correlatas será resolvida pela Liberty Health Tech.

Art. 31º Esta Resolução entra em vigor na data de sua publicação.

ANEXO I

Documento de Termo de Responsabilidade
Liberty Health Tech

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, sob pena das sanções cabíveis nos termos da (legislação vigente) que assumo a responsabilidade por:

I. Tratar o(s) ativo(s) de informação como patrimônio da Liberty Health Tech;

II. Utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço da Liberty Health Tech.;

III. Contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, sobre Estrutura de Gestão de Segurança da Informação da Liberty Health Tech;

IV. Utilizar as credenciais, as contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas da Liberty Health Tech.;

V. Responder, perante a Liberty Health Tech, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

VI. Acessar a rede corporativa, computadores, Internet e/ou utilização de e-mail, somente com autorização (usuário/senha), por necessidade de serviço ou por determinação expressa de responsável direto, realizando as tarefas e operações em estrita observância aos procedimentos, normas e disposições contidas na Resolução Normativa que rege o acesso à rede corporativa, computadores, Internet e/ou utilização de e-mail;

VII. Utilizar o correio eletrônico (*e-mail*) colocado a minha disposição somente por necessidade de serviço ou por determinação expressa de responsável direto, realizando as tarefas e operações, em estrita observância aos procedimentos, normas e disposições contidas na Resolução Normativa que rege o acesso à rede corporativa, computadores, Internet e/ou utilização de e-mail;

VIII. Não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior;

IX. Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

X. Não me ausentar da estação de trabalho sem encerrar a sessão de uso do navegador (*browser*), bloquear estação de trabalho, bem como encerrar a seção do cliente de correio, garantindo assim a impossibilidade de acesso indevido por terceiros;

XI. Não revelar minha senha de acesso à rede corporativa, computadores, Internet e/ou do correio eletrônico (e-mail) a ninguém e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento;

XII. Responder em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações a que tenha acesso.

Local,_____de_____de_____.

_____
Assinatura
Nome do usuário e seu setor organizacional

_____
Nome da autoridade responsável pela autorização do acesso

Referências Bibliográficas

GOV.BR. https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-e-modelos
Modelo de Política de Gestão de Ativos https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/modelo_politica_controle_acesso.pdf