Governo do Estado de São Paulo
Fundação Centro de Atendimento Socioeducativo ao Adolescente
ATI - Assessoria de Tecnologia da Informação

INSTRUÇÃO

Nº do Processo: 161.00063070/2025-47

Interessado: FUNDAÇÃO CASA, ATI - Assessoria de Tecnologia da Informação

Assunto: Política de Gestão de Acessos

Responsável	Assessoria de Tecnologia da Informação - ATI
Aprovado por:	Gabinete da Presidência.
Políticas Relacionadas	Política de Governança de TI, Política de Segurança da Informação, Política de Uso Aceitável de TI, Política de Gestão de Ativos de TI, Política de Backup e Recuperação de Dados.
Localização de armazenamento	Processo SEI 161.00063070/2025-47
Data da Aprovação	Data da Assinatura
Data de revisão	
Versão	1.0

1- PROPÓSITO

A Política de Gestão de Acessos objetiva estabelecer controles de identificação, autenticação e autorização para salvaguardar as informações da Fundação CASA-SP, 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.

O adequado controle do acesso é essencial para a garantia de segurança dos dados armazenados decorrentes da política de atendimento socioeducativo.

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, 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 e da rede da

Fundação CASA-SP.

2- ESCOPO

Esta Política se aplica a todas as informações, cuja a Fundação CASA-SP 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 servidores efetivos ou estagiários, da Fundação CASA-SP.

· Todos os contratados e terceiros que trabalham para a Fundação CASA-SP.

· Todos os funcionários de parceiros que acessam fisicamente as dependências ou que acessam a rede e sistemas de informação da Fundação CASA-SP.

3 - 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;

ACESSO FÍSICO - refere-se à capacidade de um indivíduo de entrar em áreas ou instalações físicas protegidas, como escritórios, data centers ou salas de servidores.

ACESSO LÓGICO - refere-se à capacidade de um usuário ou sistema de interagir com recursos tecnológicos por meio de mecanismos digitais. Inclui o uso de credenciais, autenticações e autorizações para acessar sistemas, dados e aplicações, geralmente mediado por computadores ou dispositivos conectados.

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. Via de regra, requer procedimentos de autenticação;

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

PRINCÍPIO DO MENOR PRIVILÉGIO - Limitação de acessos às permissões estritamente necessárias para a execução das funções atribuídas.

SISTEMAS EXTERNOS - Sistemas externos são aplicações, plataformas ou serviços de tecnologia da informação que não estão diretamente hospedados ou gerenciados pela infraestrutura interna da organização. Esses sistemas são normalmente fornecidos por terceiros, parceiros comerciais ou órgãos regulatórios, e podem incluir serviços baseados em nuvem, software como serviço (SaaS), portais governamentais, e soluções externas contratadas para atender a necessidades específicas da organização.

4 - REFERÊNCIAS LEGAIS E DE BOAS PRÁTICAS

Orientação	Seção
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II art. 50
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo, art.3, Inciso I
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Inciso XI CAPÍTULO VI - Seção IV – Art.15
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Instrução Normativa 01/GSI/PR	Art.12, Inciso IV, alínea f
ABNT NBR ISO/IEC 27002: 2013. Código de Prática para controles de Segurança da Informação	Itens 9 – 11.2.9 (Páginas 23 - 47)
CIS V8	CAPÍTULO 6
Guia do Framework de Privacidade e Segurança da Informação (PPSI)	Controles 5, 6, 12 e 31
Instrução Normativa Nº 04/GSI/PR, de 26 de março de 2020	Capítulo II
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra
Account and Credential Management Policy Template for CIS Controls 5 and 6	Em sua íntegra
ABNT NBR ISO/IEC 27701: 2019. Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e Diretrizes	Itens 6 – 6.6.2 (Página 16)

ISO/IEC FDIS 29151:2016(E). Information technology — Security techniques — Code of practice for personally identifiable information protection	Itens 9 – 9.2.2 e 9.2.3 (Página 11)
GSI 09/2023. OSIC (ORIENTAÇÃO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA) — Gestão de Acesso Privilegiado (Privileged Access Management – PAM) – parte 2 de 2. Disponível em: https://www.gov.br/gsi/pt-br/ssic/osic/OSIC%2009.23	Em sua íntegra

5- DECLARAÇÕES DA POLÍTICA

Dos princípios gerais:

I. A Política de Gestão de Acessos deve estar alinhada com à Política de Segurança da Informação da Fundação CASA-SP.

II. A Política de Gestão de Acessos deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

Art. 1º Fica aprovada, no âmbito da Fundação CASA-SP, a Política para Criação e Administração de contas de acesso, em complemento às diretrizes estabelecidas pelo Capítulo II, da Política de Segurança da Informação - PSI da Fundação CASA-SP.

Art. 2° A Fundação CASA-SP deve definir regras de limitação ou restrição de acesso aos colaboradores, para que estes disponham de privilégios mínimos necessários para exercerem suas atividades, funções e responsabilidades pré-definidas.

CAPÍTULO I - ACESSO LÓGICO

Art. 3º O acesso lógico aos recursos da Rede Local deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pela Seção de Segurança da Informação, baseado nas responsabilidades e tarefas de cada usuário.

I. A Seção de Segurança da Informação deve implementar protocolos de comunicação e redes seguros.

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

III. Para fins desta Política, consideram-se usuários de recursos de tecnologia da informação servidores ocupantes de cargo efetivo ou cargo em comissão, assim como funcionários de empresas prestadoras de serviços, estagiários e demais usuários temporários em atividade na Fundação CASA-SP.

IV. O acesso remoto deve ser realizado por meio de VPN – Rede Virtual Privada, após as devidas autorizações.

V. Recomenda-se a utilização de MFA para a autenticação de acesso remoto, sempre que houver disponibilidade de licença e orçamento.

VI. O acesso a todas as aplicações corporativas ou de terceiros que estejam hospedados em

fornecedores deve utilizar MFA.

VII. A Seção de Segurança da Informação deve centralizar a autenticação, autorização e auditoria (AAA) dos ativos de informação da sua infraestrutura de rede.

VIII. A Seção de Segurança da Informação deve planejar a adoção técnicas de segmentação de rede visando limitar o acesso de forma eficiente e segura, assegurando que apenas colaboradores e dispositivos autorizados possam interagir com partes específicas da rede.

Art. 4º A Seção de Segurança da Informação é responsável por validar todas as contas ativas da Fundação CASA-SP a cada 90 dias.

Art. 5º A Seção de Segurança da Informação deve implementar a centralização da gestão de contas por meio de serviço de diretório e/ou identidade.

Art. 6º A Seção de Segurança da Informação deve estabelecer e manter um inventário dos sistemas de autenticação e autorização da Fundação CASA-SP, tal inventário deve ser revisado periodicamente.

Art. 7º A Seção de Segurança da Informação deve centralizar o controle de acesso para todos os ativos de informação da organização por meio de um serviço de diretório ou provedor de SSO.

Art. 8º A Seção de Segurança da Informação deve definir e manter o controle de acesso dos usuários baseado em funções.

I. Deve ser elaborada a documentação dos direitos dos acessos para cada função dentro da Fundação CASA-SP.

II. A Seção de Segurança da Informação deverá realizar 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.

III. Ao conceder acesso a usuários que lidam com dados pessoais, deve-se limitar, estritamente, o acesso aos sistemas que processam esses dados ao mínimo necessário para cumprir os objetivos essenciais do processamento, em conformidade com o princípio do menor privilégio. Ao atribuir ou revogar os direitos de acesso concedidos deve-se incluir:

a) Verificação de que o nível de acesso concedido é apropriado às políticas de acesso, além de ser consistente com outros requisitos, tais como, segregação de funções;

b) Garantia de que os direitos de acesso não estão ativados antes que o procedimento de autorização esteja completo;

c) Manutenção de um registro preciso e atualizado dos perfis dos usuários criados para os que tenham sido autorizados a acessar o sistema de informação e os dados pessoais neles contidos;

d) Mudança dos direitos de acesso dos usuários que tenham mudado de função ou de atividades, e imediata remoção ou bloqueio dos direitos de acesso dos usuários que deixaram a Fundação CASA-SP;

e) Analisar criticamente os direitos de acesso em intervalos regulares.

Art. 9º A Seção de Segurança da Informação deve implementar um processo formal de registro de usuários que tratem de dados pessoais para permitir atribuição de direitos de acesso e fornecer medidas para lidar com o comprometimento do controle de acesso do usuário, como corrupção ou comprometimento de senhas ou outros dados de registro do usuário, para tanto podem ser

realizadas as seguintes ações:

I. O uso de um identificador de usuário único, para permitir relacionar os usuários com suas responsabilidades e ações;

II. O uso compartilhado de identificador de usuário somente será permitido, onde eles são necessários por razões operacionais ou de negócios e deverá ser aprovado e documentado;

III. A garantia de que o um mesmo identificador de usuário não é emitido para outros.

Art. 10º Os gestores unidades organizacionais responsáveis pelos sistemas e pastas de rede deverão:

I. Definir os padrões de acesso com base nas atribuições gerais dos cargos e na lotação dos servidores;

II. Estabelecer critérios claros para a concessão de acessos, levando em consideração as atividades desempenhadas pelo servidor;

III. Autorizar qualquer necessidade de concessão de acesso fora dos padrões definidos, indicando prazo para revogação do acesso;

IV. Realizar avaliações periódicas dos perfis e privilégios de acesso dos sistemas e pastas de rede sob sua responsabilidade e dos usuários lotados em suas unidades organizacionais, de modo a assegurar que estes estejam estritamente alinhados às funções desempenhadas e às necessidades operacionais

Art. 11 A concessão de acessos a sistemas e pastas de rede será feita conforme os seguintes critérios:

I. Cargo: Os acessos serão determinados com base nas atribuições do cargo ou função do servidor;

II. Lotação: O local de lotação do servidor poderá determinar níveis específicos de acesso, de acordo com as necessidades da unidade;

III. Excepcionalidades: Nos casos em que o padrão de acesso não seja suficiente, o gestor da unidade poderá solicitar acessos excepcionais mediante justificativa formal e prazo definido.

CAPÍTULO II -CONTA DE ACESSO LÓGICO E SENHA

Art. 12 Para utilização das estações de trabalho da Fundação CASA-SP, será obrigatório o uso de uma única identificação (*login*) e de senha de acesso, fornecidos pela Seção de Segurança da Informação, mediante solicitação formal pelo titular da unidade do requisitante.

I. A solicitação de acessos deve ser realizada no sistema ATI - Tarefas.

II. Os privilégios de acesso dos usuários à Rede Local devem ser definidos pelo gestor da unidade 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 gestor da unidade do usuário deverá encaminhar solicitação para a Seção de Segurança da Informação, por meio do ATI – Tarefas, que a examinará, podendo negá-la nos casos em que a entender desnecessária.

Parágrafo único. Os sistemas desenvolvidos pela Fundação CASA-SP utilizarão exclusivamente essa conta de acesso.

Art. 13 O *login* e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados pela Seção de Segurança da Informação quando constatada qualquer irregularidade.

Parágrafo único. Para retomar o acesso à rede, deverá ser formalizada nova requisição pelo titular da unidade do requisitante.

Art. 14 O padrão adotado para o formato da conta de acesso do usuário é a sequência primeiro nome + iniciais dos sobrenomes.

Parágrafo único. Nos casos de já existência de conta de acesso para outro usuário, a Seção de Segurança da Informação realizará outra combinação para o qual a conta está sendo criada.

Art. 15 O padrão adotado para o formato da senha é o definido pela Seção de Segurança da Informação, 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 Local deve seguir as regras de:

a) Possuir tamanho mínimo de 8 caracteres;

b) Conter pelo menos uma letra maiúscula;

c) Conter pelo menos uma letra minúscula;

d) Conter números;

e) Conter símbolos, incluindo: ! @ # $ % ^ & * - _ + = [ ] { } | \ : ‘ , . ? / ` ~ “ < > ( );

f) 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;

g) Não utilizar termos óbvios, tais como: Brasil, senha, usuário, *password* ou *system*.

h) Não reutilizar as últimas 2 senhas.

II. A Seção de Segurança da Informação 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 Local.

Art. 16 As senhas de acesso serão renovadas a cada 120 dias, devendo o usuário ser informado antecipadamente a fim de que ele próprio efetue a mudança.

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

CAPÍTULO III -BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE ACESSO

Art. 17 A conta de acesso será bloqueada nos seguintes casos:

I. Após 5 tentativas consecutivas de acesso errado;

II. Solicitação do superior imediato do usuário com a devida justificativa;

III. Quando da suspeita de mau uso dos serviços disponibilizados pela Fundação CASA-SP ou

descumprimento da Política de Segurança da Informação – PSI e normas correlatas em vigência.

IV. Após 180 dias consecutivos sem movimentação pelo usuário interno ou externo.

Art. 18 Nos casos dos incisos II e III do Art. 15, o desbloqueio da conta de acesso à Rede Local será realizado apenas após solicitação formal do superior imediato do usuário à Seção de Segurança da Informação, devendo nos demais casos o usuário entrar em contato com a Seção de Atendimento ao Usuário.

Art. 19 A Seção de Segurança da Informação deve garantir a implementação de um processo formal de cancelamento de usuários que administrem ou operem sistemas e serviços que tratem de dados pessoais. Tal processo deverá incluir a imediata remoção ou desabilitação de usuário que tenha deixado a Fundação CASA.

Art. 20 A Seção de Segurança da Informação pode configurar o bloqueio automático de sessão nos ativos após um período de inatividade preestabelecido.

Art. 21 A Seção de Segurança da Informação deve, sempre que possível, priorizar a revogação/desativação de contas com o objetivo de manter dados e logs para possíveis auditorias.

CAPÍTULO IV - ACESSO FÍSICO

Art. 22 A Gerência de Infraestrutura e Segurança da Informação deve definir perímetros de segurança para proteger ambientes e ativos contra acesso físico não autorizado, danos e interferências de acordo com as diretrizes a seguir:

I. Definir a localização e resistência dos perímetros de acordo com os requisitos de segurança da informação relacionados aos ativos que se encontre dentro dos perímetros.

II. Proteger os ambientes seguros contra acessos não autorizados por meio de mecanismos de controle de acesso, como fechaduras tradicionais ou digitais, que possibilitem autenticação por biometria, senhas, PINS ou cartões de acesso.

a) A Gerência de Infraestrutura e Segurança da Informação deve executar testes nos mecanismos de controle de acesso em períodos pré-definidos para assegurar a funcionalidade total do equipamento.

b) Os mecanismos de controle de acesso devem ser monitorados pela Seção de Segurança da Informação.

III. Estabelecer uma área de recepção ou outros meios de controle de acesso físico a ambientes que não for conveniente a implementação de mecanismos de controle de acesso.

Art. 23 O acesso físico a ambientes seguros ou ativos de tratamento e armazenamento de dados da Fundação CASA-SP é destinado apenas a pessoal autorizado.

Art. 24 A Gerência de Infraestrutura e Segurança da Informação deve manter um processo de gestão de acessos para fornecimento, revisão periódica, atualização e revogação das autorizações.

Art. 25 A Gerência de Infraestrutura e Segurança da Informação deve implementar e manter seguro logs ou registro físico de todos os acessos aos ativos de informação.

Art. 26 O acesso a ambientes seguros ou ativos de tratamento e armazenamento de dados por fornecedores ou prestadores de serviços será concedido somente quando necessário e de acordo com as seguintes diretrizes:

I. Para fins específicos e autorizados;

II. Autorização concedida pela Gerência de Infraestrutura e Segurança da Informação;

III. Supervisionado e monitorado.

Art. 27 Os ativos de armazenamento e tratamento de dados que se encontrem fora da Fundação CASA-SP devem ser protegidos contra perda, roubos, danos e acesso físico não autorizados conforme as seguintes diretrizes:

I. Não deixar o ativo sem vigilância em locais públicos e inseguros;

II. Proteger o ativo contra riscos associados a visualização de informações por outra pessoa;

III. Implementar as funcionalidades de rastreamento e limpeza remota.

Art. 28 A **Política de Gestão de Ativos de TI** e a **Política de Backup e Recuperação de Dados** abordarão sobre a gestão de mídias de armazenamento, de acordo com as seguintes diretrizes:

I. Exigir autorização para a saída de mídias de armazenamento da Fundação CASA-SP;

II. Armazenar mídias em local seguro de acordo com a classificação de suas informações;

III. Manter cópias de segurança de mídias de acordo com a classificação de suas informações.

Art. 29 A **Política de Uso Aceitável de TI** definirá condições e restrições pertinentes ao acesso físico nos dispositivos de trabalho remoto, levando em consideração as seguintes diretrizes:

I. Segurança física do local de trabalho remoto;

II. Regras e orientações quanto ao acesso de familiares e visitantes ao dispositivo.

CAPÍTULO V - MOVIMENTAÇÃO INTERNA

Art. 30 Quando houver mudança do usuário para outro setor ou o usuário ocupar uma nova função, os direitos de acesso à Rede Local devem ser revogados.

I. O novo superior imediato deve realizar a solicitação de novos acessos de acordo com novo setor / função do usuário.

II. Os direitos de acesso antigos devem ser imediatamente cancelados conforme solicitação do antigo superior imediato ou da Divisão de Recursos Humanos – DRH.

CAPÍTULO VI - CONTA DE ACESSO BIOMÉTRICO

Art. 31 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 Fundação CASA-SP deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

CAPÍTULO VI - ASSESSOS EM SISTEMAS EXTERNOS

Art. 32 Os acessos a sistemas externos devem ser gerenciados com o mesmo rigor aplicado aos sistemas internos, assegurando alinhamento às boas práticas de segurança e conformidade regulatória.

Art. 33 Os acessos a sistemas externos devem ser atribuídos individualmente, sendo vedado o uso de contas genéricas ou compartilhadas.

Art. 34 As aprovações e gestão dos usuários devem ser realizadas por gestores responsáveis pela área ou pelo sistema externo.

CAPÍTULO VII - ADMINISTRADORES

Art. 35 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 da Gerência de Infraestrutura e Segurança da Informação e da Gerência de Suporte ao Usuário, 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 Seção de Segurança da Informação, 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, não podendo instalar, desinstalar ou remover qualquer programa sem autorização formal da Seção de Suporte Técnico, a qual é responsável em conjunto com a Seção de Segurança da Informação pela homologação de sistemas.

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

V. A identificação (*login*) com privilégio de administrador nos equipamentos locais será fornecida em caráter provisório, podendo ser renovada por solicitação formal do titular da unidade requisitante.

VI. Salvo para atividades específicas da área responsável pela gestão da tecnologia da informação do órgão, não será concedida, para um mesmo usuário, identificação (login) com privilégio de administrador para mais de uma estação de trabalho, ou para acesso a equipamentos servidores e a dispositivos de rede.

VII. Excepcionalmente, poderão ser concedidas identificações (*login*) de acesso à rede de comunicação de dados a visitante em caráter temporário após apreciação da Seção de Segurança da Informação.

VIII. A Seção de Segurança da Informação deve restringir os privilégios de administrador a contas de administrador dedicados nos ativos de informação, para que o usuário com privilégio de administrador não consiga realizar atividades gerais de computação, como navegação na Internet, e-mail e uso do pacote de produtividade, estas atividades deverão ser realizadas preferencialmente a partir da conta primária não privilegiada do usuário.

IX. Ao tratar dados pessoais a Fundação CASA-SP deve observar o princípio do privilégio mínimo como regra, para garantir que o usuário receba apenas os direitos mínimos necessários para executar suas atividades, para tanto podem ser realizadas as seguintes ações:

a) Remover os direitos de administrador nos dispositivos finais;

b) Remover todos os direitos de acesso root e admin aos servidores e utilizar tecnologias que permitam a elevação granular de privilégios conforme a necessidade, ao mesmo tempo em que

fornecem recursos claros de auditoria e monitoramento;

c) Eliminar privilégios permanentes (privilégios que estão “sempre ativos”) sempre que possível;

d) Limitar a associação de uma conta privilegiada ao menor número possível de pessoas;

e) Minimizar o número de direitos para cada conta privilegiada.

CAPÍTULO VIII - RESPONSABILIDADES

Art. 36 É de responsabilidade da Divisão de Recursos Humanos comunicar à Seção de Segurança da Informação o desligamento do usuário da Fundação CASA-SP, inclusive estagiários, para que as permissões de acesso à Rede Local e recursos sejam cancelados.

Art. 37 É responsabilidade do Gestor do Contrato ou Parceria da Fundação CASA-SP a comunicação imediata à Seção de Segurança da Informação sobre desligamentos, férias e licenças de funcionários de empresas prestadoras de serviços, para que seja efetuado o bloqueio momentâneo ou revogação definitiva da permissão de acesso aos recursos.

Art. 38 Os serviços serão filtrados por programas de *antivírus*, *anti-phishing* e *anti*-spam e, caso violem alguma regra de configuração, serão bloqueados ou excluídos automaticamente.

Art. 39 É de responsabilidade da Seção de Segurança da Informação o monitoramento da utilização de serviços de rede e de acesso à Internet, podendo ainda exercer fiscalização nos casos de apuração de uso indevido desses recursos, bem como bloquear, temporariamente, sem aviso prévio, a estação de trabalho que esteja realizando atividade que coloque em risco a segurança da rede, até que seja verificada a situação e descartada qualquer hipótese de dano à infraestrutura tecnológica da Fundação CASA-SP.

Art. 40 O usuário é responsável por todos os acessos realizados através de sua conta de acesso e por possíveis danos causados à Rede Local e a recursos de tecnologia custodiados ou de propriedade da Fundação CASA-SP.

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 Local em mais de uma estação de trabalho ou notebook deve ser evitada, 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 à Rede Local.

IV. É dever do usuário informar à Assessoria de Tecnologia da Informação se estiver habilitado para ele algum acesso que não condiz com as suas atribuições e responsabilidades.

Art. 41 O usuário deve informar à Assessoria de Tecnologia da Informação qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.

Art. 42 É dever do 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 (Modelo – Anexo I) quanto a utilização da respectiva conta de acesso.

CAPÍTULO IX - DISPOSIÇÕES GERAIS

Art. 43 As aplicações não devem armazenar a senha do USUÁRIO, mas sim utilizar o hash criptográfico da mesma, sendo recomendado o uso do algoritmo SHA 256 ou superior.

Art. 44 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 à Assessoria de Tecnologia da Informação.

Art. 45 Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, a Gerência de Infraestrutura e Segurança da Informação fará a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.

I. Nos casos em que o ator da quebra de segurança for um usuário, a Assessoria de Tecnologia da Informação comunicará os resultados ao superior imediato do mesmo para adoção de medidas cabíveis.

II. Ações que violem a PSI 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. Processo administrativo disciplinar específico deverá ser instaurado para apurar as ações que constituem em quebra das diretrizes impostas por esta Norma e pela PSI.

IV. A resolução de casos de violação/transgressões omissos nas legislações correlatas será resolvida pelo Gabinete da Presidência da Fundação CASA-SP.

Art. 46 O acesso à conta de e-mail será detalhado na Política de Serviços de Mensageria e Telefonia.

Art. 47 Esta Política entra em vigor na data de sua publicação.

ANEXO I

Modelo de Termo de Responsabilidade

Fundação CASA-SP

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, em _____, e lotado no(a)_____desta Fundação CASA-SP, DECLARO , 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 Fundação CASA-SP;

II. Utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço da Fundação CASA-SP.;

III. Contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

IV. Utilizar as credenciais, as contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas da Fundação CASA-SP.;

V. Responder, perante a Fundação CASA-SP, 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 superior hierárquico, realizando as tarefas e operações em estrita observância aos procedimentos, normas e disposições contidas na Política de Segurança da Informação e demais normas e procedimentos em segurança da informação que regem 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 superior hierárquico, 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.

XIII. Declaro ter conhecimento das Políticas abaixo e concordo em aceitar suas regras.

a. Política de Backup e Recuperação de Dados

b. Política de Continuidade Operacional de TI

c. Política de Gestão de Acessos

d. Política de Gestão de Ativos de TI

e. Política de Gestão de Capacidade e Desempenho

f. Política de Gestão de Incidentes e Problemas

g. Política de Gestão de Mudanças

h. Política de Gestão de Serviços de TI

i. Política de Proteção de Dados e Privacidade

j. Política de Segurança da Informação

k. Política de Serviços de Mensageria e Telefonia

I. Política de Uso Aceitável de TI

XIV. Declaro estar ciente de que minhas ações serão monitoradas de acordo com a Política de Segurança da Informação e de que qualquer alteração feita sob minha identificação, advinda de minha autenticação e autorização, é de minha responsabilidade.

Local, SP, _____de _____de _____.

_____

Assinatura

Nome do usuário e seu setor organizacional

Nome da autoridade responsável pela autorização do acesso

São Paulo, na data da assinatura digital.

Raelen Bego Luiz
Chefe de Gabinete

Leandro Timossi de Almeida
Assessor da Presidência

Documento assinado eletronicamente por **Leandro Timossi de Almeida**, **Assessor da Presidência II**, em 13/03/2025, às 16:33, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Raelen Bego Luiz**, **Chefe de Gabinete**, em 18/03/2025, às 22:30, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

A autenticidade deste documento pode ser conferida no site https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0059070679** e o código CRC **5C3EA7D6**.