TecnoTech
Sistemas

POLÍTICA DE CONTROLE DE ACESSO LÓGICO

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Tecnotech Sistemas

Felipe Santos de Andrade / Wanderson Camara dos Santos

Política de uso da internet corporativa

Versão 1.0

Tecnotech Sistemas

Diretoria de Implementação e Projetos

Política criada sob a supervisão de

Romney Dutra / Lucas Diniz - Prolinx

Março de 2023

Abreviaturas e siglas

Acesso lógico: Direito de acesso na modalidade virtual a um ativo de tecnologia da informação.

Acesso lógico privilegiado: Acesso lógico privilegiado é um tipo específico de acesso à aplicação de infraestrutura computacional ou de configuração de serviços em ativos de tecnologia da informação sob responsabilidade da tecnotech sistemas, incluindo: sistema gerenciador de banco de dados, acesso remoto a servidores, configuração de micro serviços e acesso à serviço que trata dados pessoais.

Ativo de tecnologia da informação: Recurso digital que constitui um sistema de informação, tais como: dados, serviço de conectividade, informação e programas de computador.

Cancelamento de usuário: Processo para desabilitar a credencial de um usuário.

Controle de acesso lógico: Operação de conceder, alterar, analisar e revogar direito de acesso a um ativo de tecnologia da informação.

Gestão de usuário: Operações de cadastro, alteração, análise ou cancelamento de usuário.

Passe: Padrão de controle criado a partir de algo que somente o usuário tem, é, ou sabe, para confirmar a identidade do respectivo usuário ao ativo de tecnologia da informação.

Abreviaturas e siglas

Processo de negócio: Conjunto de atividades ou tarefas estruturadas para produção de um resultado de valor para o cliente, por meio da entrega de um serviço ou produto, conduzidos por uma unidade ou setor.

Regras de negócios: Declarações sobre a forma de operar um processo de negócio ou uma rotina.

Revogação de acesso: Cancelamento do direito de acesso lógico do usuário a um ativo de tecnologia de informação.

Setor: Unidade da estrutura organizacional da Tecnotech Sistemas.

Senha: Conjunto de caracteres secretos utilizado como sinal de reconhecimento de uma pessoa - ou, padrão de controle que somente o usuário sabe.

Usuário: Identificação de uma pessoa na base de dados de um sistema por meio de um identificador único denominado "nome de usuário" para o qual pode ser associado direito de acesso lógico. Acesso autenticado: Acesso restrito que exige a identificação da pessoa, por meio do usuário e passe, para acessar um serviço de tecnologia da informação.

Conteúdo

Lista de Tabelas

Capítulo 1

INTRODUÇÃO

Este documento tem como objetivo estabelecer um conjunto de regras para controle do acesso lógico aos ativos de tecnologia da informação na tecnotech Sistemas.

Capítulo 2

ABRANGÊNCIA

Obedecer às regras e orientações deste documento é fundamental para todos que atuam em nome da tecnotech sistemas, incluindo Diretores, Funcionários, Estagiários, Parceiros Comerciais (consultores, agentes comerciais e conveniados) e pessoas externas que usam serviços de tecnologia da informação da Tecnotech, com acesso restrito (acesso autenticado).

Capítulo 3

OBJETIVO

Este documento da tecnotech tem como propósito estabelecer um conjunto de diretrizes para o gerenciamento de regras para controle do acesso lógico aos ativos de tecnologia da informação, com o objetivo de minimizar riscos na gestão de credenciais de acesso lógico. As normas definidas buscam atingir objetivos específicos, tais como:

- Definir um conjunto mínimo de regras de controle de acesso lógico para proteger os recursos de tecnologia da informação contra acessos não autorizados.
- Estabelecer um procedimento para atribuição clara de responsabilidades aos usuários de forma a validar o processo.
- Definir um conjunto mínimo de procedimentos para controlar o acesso lógico aos recursos de tecnologia da informação.

Capítulo 4

TRATAMENTO DE INCIDENTES

Para garantir a eficácia da política de controle de acesso lógico, adotamos controles de segurança da informação e de privacidade de dados onde possui medidas para lidar com possíveis incidentes de segurança e violações, esse processo pode ser visualizado em nossa política de segurança da informação e na política de privacidade de dados, essa última publicada através do link https://wiki.app.sitac.com.br/books/politica-de-resposta-a-incidentes .

- **A falta de implementação de padrões de controle de acesso lógico baseados em algo que somente o usuário tem ou sabe deve ser considerada como um incidente de segurança.**
- **O registro de um pedido de auditoria de usuário em um determinado serviço de TI deve ser realizado pelo grupo de investigação de incidentes da tecnotech sistemas.**

Capítulo 5

RESPONSABILIDADE DA EQUIPE DE RESPOSTA A INCIDENTES

A equipe de resposta a incidentes é responsável por coordenar a resposta da tecnotech diante de um Incidente de Segurança da Informação. Suas responsabilidades incluem:

- Receber as notificações de Incidentes e realizar uma análise preliminar.
- Avaliar a gravidade do Incidente e adotar as medidas necessárias para conter, erradicar seus efeitos.
- Garantir a preservação da integridade dos Dados Pessoais afetados pelo Incidente.
- Manter registro de todos os Incidentes de Segurança da Informação ocorridos na Empresa, bem como das medidas adotadas para sua solução e contenção.
- Monitorar a eficácia das medidas de segurança da informação adotadas pela Empresa e Realizar ajustes quando necessário.
- O registrar e auditar pedidos de usuário em um determinado serviço de TI para tratamento de incidentes.

Capítulo 6

RESPONSABILIDADES DOS ENVOLVIDOS

A responsabilidade de garantir a aplicação das normas de controle de acesso lógico aos ativos de tecnologia da informação cabe à Tecnotech sistemas.

A definição dos direitos de acesso dos usuários aos ativos de tecnologia da informação tratados ou gerenciados pela Tecnotech sistemas devem ser estabelecida por ela mesma.

Para obter o direito de acesso lógico necessário para realizar as atividades na tecnotech sistemas, é preciso obter a aprovação ou validação do diretor ou gerente responsável pelo setor, em que o usuário irá atuar.

Capítulo 7

O CONTROLE DE ACESSO LÓGICO A ATIVO DE TECNOLOGIA DA INFORMAÇÃO É EXECUTADA

Quando o direito de acesso lógico é concedido pela área responsável para determinado serviço, significa que apenas os processos ou serviços gerenciados por essa área podem ser acessados. Isso ocorre porque cada área é responsável por gerenciar um conjunto específico de processos ou serviços, é a única que possui o conhecimento e a expertise necessária para controlar o acesso a esses recursos de forma segura e eficiente. Dessa forma, a concessão de direitos de acesso lógico fica restrita aos processos ou serviços gerenciados pela área responsável, garantindo a proteção dos ativos de tecnologia da informação e a privacidade das informações dos usuários. A concessão do direito de acesso lógico é baseada em critérios predefinidos, que determinam quem tem acesso a quais recursos de tecnologia da informação. Esses critérios são definidos pela tecnotech sistemas e devem ser seguidos para garantir a segurança dos ativos de tecnologia da informação e a privacidade das informações dos usuários. Quando o direito de acesso lógico é concedido, os usuários não precisam solicitar acesso individualmente, pois já fazem parte do grupo com direito a acessar determinados recursos.

Capítulo 8

GESTÃO DE USUÁRIO É EXECUTADA

Quando a tecnotech sistemas é responsável pelo acesso lógico, isso ocorre em situações em que o tratamento dos dados pessoais do usuário não é realizado em um processo meio ou finalístico da empresa. A tecnotech sistemas é a única autorizada a registrar o usuário para que ele possa ter acesso aos recursos de tecnologia da informação. Nesses casos, a tecnotech é responsável por garantir que o acesso aos recursos seja concedido de forma segura e adequada, e que as informações pessoais dos usuários sejam protegidas. Isso pode incluir a criação de políticas de segurança, e a realização de auditorias regulares para garantir a conformidade com as normas e regulamentações aplicáveis.Quando o acesso lógico é concedido pela área responsável pelo serviço, isso ocorre quando uma pessoa ainda não tem um usuário registrado na base centralizada, para autenticação de usuários é a respectiva área responsável pelo processo no qual a pessoa terá sua primeira interação com um processo da empresa. A área é responsável por conceder acesso aos recursos de tecnologia da informação necessários para que a pessoa possa interagir com o processo em questão. Isso pode envolver a criação de uma conta de usuário temporária, a atribuição de direitos de acesso específicos e a implementação de medidas de segurança adequadas para proteger as informações pessoais da pessoa. A concessão de direitos de acesso lógico nesses casos deve seguir as políticas e normas estabelecidas pela tecnotech, para garantir a segurança e a privacidade das informações.

Capítulo 9

GESTÃO DE USUÁRIOS E O CONTROLE DE ACESSO LÓGICO

- **Por fornece as ferramentas necessárias para gerenciar os usuários e controlar o acesso lógico deles, essas ferramentas incluem sistemas de autenticação, permissões de acesso e outras.**
- **É importante buscar continuamente melhorias nos processos de autenticação e controle de acesso lógico, visando aprimorar a eficiência e a segurança desses sistemas.**
- **Ajudar os setores responsáveis pelos serviços a gerenciar os usuários e fornecer treinamentos quando necessário.**
- **MDivulgar e conscientizar os usuários em seus setores na tecnotech sobre a política de controle de acesso lógico.**
- **Essa política estabelece que todos os sistemas de informação e serviços digitais mantidos, adquiridos ou desenvolvidos pela tecnotech sistemas devem utilizar o controle de acesso lógico, priorizando o uso da base de dados centralizada para autenticação.**

- **Para garantir a segurança dos ativos de tecnologia da informação, é imprescindível que as informações referentes aos direitos de acesso lógico estejam disponíveis para os responsáveis pelo tratamento de dados e pela chefia imediata dos usuários. Essas informações incluem a:**
- **Identificação dos usuários ou grupos de usuários que possuem acesso lógico ao ativo de TI.**
- **Níveis de privilégios de acesso para cada usuário ou grupo de usuários.**
- **Regras de uso e restrições de acesso, quando aplicáveis.**

9.1 ACESSO ÀS REDES E AOS SERVIÇOS DE REDE

- **A concessão de acesso lógico à rede e aos serviços de rede deve ser feita somente a usuários previamente autorizados.**
- **A identificação do acesso lógico e atividades do usuário devem ser registradas para auxiliar na responsabilização das ações do usuário.**

Capítulo 10

REGISTRO E CANCELAMENTO DE USUÁRIO

- Cada funcionário tem somente uma identificação de usuário ativa nos sistemas de informação e serviços da tecnotech sistemas.
- Todos os usuários atestam conhecimento sobre suas responsabilidades em relação à Segurança das Informações e da criação e uso de senhas da tecnotech, após a assinatura no termo de compromisso e confidencialidade e na política de criação e uso de senhas.
- Para garantir a segurança dos sistemas e das informações confidenciais, é importante que as senhas sejam alteradas regularmente.
- O uso compartilhado de usuário é permitido somente pela diretoria quando este é necessário por razões específicas de um processo desde que:
- Esteja formalmente documentado e com responsabilização do gestor do processo de negócio.

- **No caso de término do vínculo do usuário com a tecnotech sistemas, o cancelamento de todos os direitos de acesso vigentes do usuário deve ocorrer de forma imediata, geral em todos os ativos de tecnologia da informação, quando a pessoa encerrar o vínculo, é importante lembrar que o usuário deve devolver todos os dispositivos e equipamentos de propriedade da empresa que possam conter informações confidenciais.**

- **A gestão de usuário e passe para acesso a ativos de tecnologia da informação devem estar em conformidade com a Política de criação e uso de senhas, quando o controle de acesso lógico usar senhas, independentemente do sistema de autenticação utilizado.**

- **A gestão de usuário deve considerar que:**

- **O usuário não pode ser excluído, ele deve ser inativado ou desabilitado.**

- **A inativação de usuário deve existir quando houver regras de bem definidas e implementações viáveis em programa de computador.**

- **A inativação pode fundamentar-se, também, em análise crítica que apresenta o risco do usuário ativo à segurança da informação, ou desconformidade com algum normativo vigente.**

- **para garantir a segurança da informação, é importante que o controle de acesso lógico (mecanismo que gerencia o acesso de usuários a um sistema ou rede) utilize uma base centralizada para autenticar os usuários. Essa base centralizada é responsável por verificar se o usuário possui as credenciais corretas (como nome de usuário e senha) para acessar sistemas ou rede.**

Capítulo 11

FORNECER ACESSO AO USUÁRIO

- **Para garantir a segurança e a proteção das informações em um ambiente de tecnologia da informação, é essencial que a concessão de acesso lógico seja realizada somente com a autorização ou consentimento do responsável que gerencia o ativo a ser acessado. Dessa forma, é possível evitar o acesso não autorizado e manter a integridade dos dados.**

- **É fundamental que a concessão de acesso lógico esteja em total conformidade com as políticas, normas e procedimentos da empresa relacionados à segurança da informação e privacidade de dados. A observância dessas diretrizes garante a proteção das informações e dados confidenciais, prevenindo o acesso indevido e mitigando potenciais riscos de segurança. É importante destacar que as políticas e normas devem ser aplicadas de forma consistente e atualizadas regularmente para se adequar às constantes mudanças tecnológicas e de segurança.**

- **Para garantir uma gestão efetiva e segura do acesso lógico dos usuários, é crucial que o processo seja padronizado e amplamente divulgado pelo gestor de tecnologia da informação e pela área de negócio responsável pelo registro dos usuários. A padronização do processo ajuda a evitar erros e inconsistências na concessão de acesso, além de facilitar a manutenção e atualização das informações. É importante que as informações sejam publicadas de forma clara e objetiva, de modo a promover a transparência e permitir que os usuários entendam facilmente as regras e procedimentos de acesso. Dessa forma, a organização poderá garantir uma gestão eficiente e segura do acesso lógico aos seus sistemas e dados.**
- **O provisionamento de acesso lógico dos usuários que tiverem sua função, atividade ou projetos alterados, as seguintes ações devem ser tomadas:**
- **A diretoria deve comunicar formalmente a alteração ao setor responsável pela gestão do acesso lógico concedido à respectiva pessoa.**
- **O nível de acesso lógico deve ser revogado ou readequado à nova situação funcional.**
- **Os direitos de acesso de um usuário devem ser revisados periodicamente e ajustados de acordo com mudanças.**
- **Caso o usuário mude seu vínculo com a tecnotech sistemas, será necessário revogar seu acesso lógico aos ativos de tecnologia da informação concedidos ao vínculo anterior. Isso se deve ao fato de que o acesso lógico é concedido com base nas atribuições e responsabilidades do usuário dentro da empresa, e essas informações são diretamente relacionadas ao seu vínculo com a tecnotech sistemas.**
- **Os direitos de acesso lógico concedidos após mudança de vínculo serão tratados em procedimentos específicos pelos diretores.**
- **Os direitos de acesso lógico aos ativos de tecnologia da informação devem ser analisados criticamente em intervalos de 12 meses, no máximo, pelos gestores e pelas chefias imediatas dos usuários para os quais há concessão de acesso lógico.**

Capítulo 12

GERENCIAMENTO DO DIREITO DE ACESSO LÓGICO PRIVILEGIADO

A gestão de direitos de acesso lógico privilegiado deve atender requisitos complementares, tais como:

- **Não remover acessos lógico privilegiado sem confirmar a necessidade de manter o respectivo acesso para o usuário.**
- **Usar login único ou manter usuários com acesso privilegiado ao ambiente de infraestrutura computacional com login de usuário e senhas aos sistemas da empresa.**

Capítulo 13

GERENCIAMENTO DA INFORMAÇÃO DE AUTENTICAÇÃO SECRETA DE USUÁRIO

- **A complexidade mínima para as credenciais armazenadas e a temporalidade para a sua alteração devem seguir as normas definidas pela tecnotech sistemas, conter pelo menos uma letra maiúscula, conter pelo menos uma letra minúscula, conter números (0 a 9), conter símbolos, tamanho de no mínimo 8 caracteres.**
- **Informações sensíveis como senhas ou tokens de acesso devem ser armazenadas de forma criptografada e medidas de segurança devem garantir que apenas usuários autorizados tenham acesso ao cadastro.**

Capítulo 14

FLUXOGRAMA DE ACESSO LÓGICO

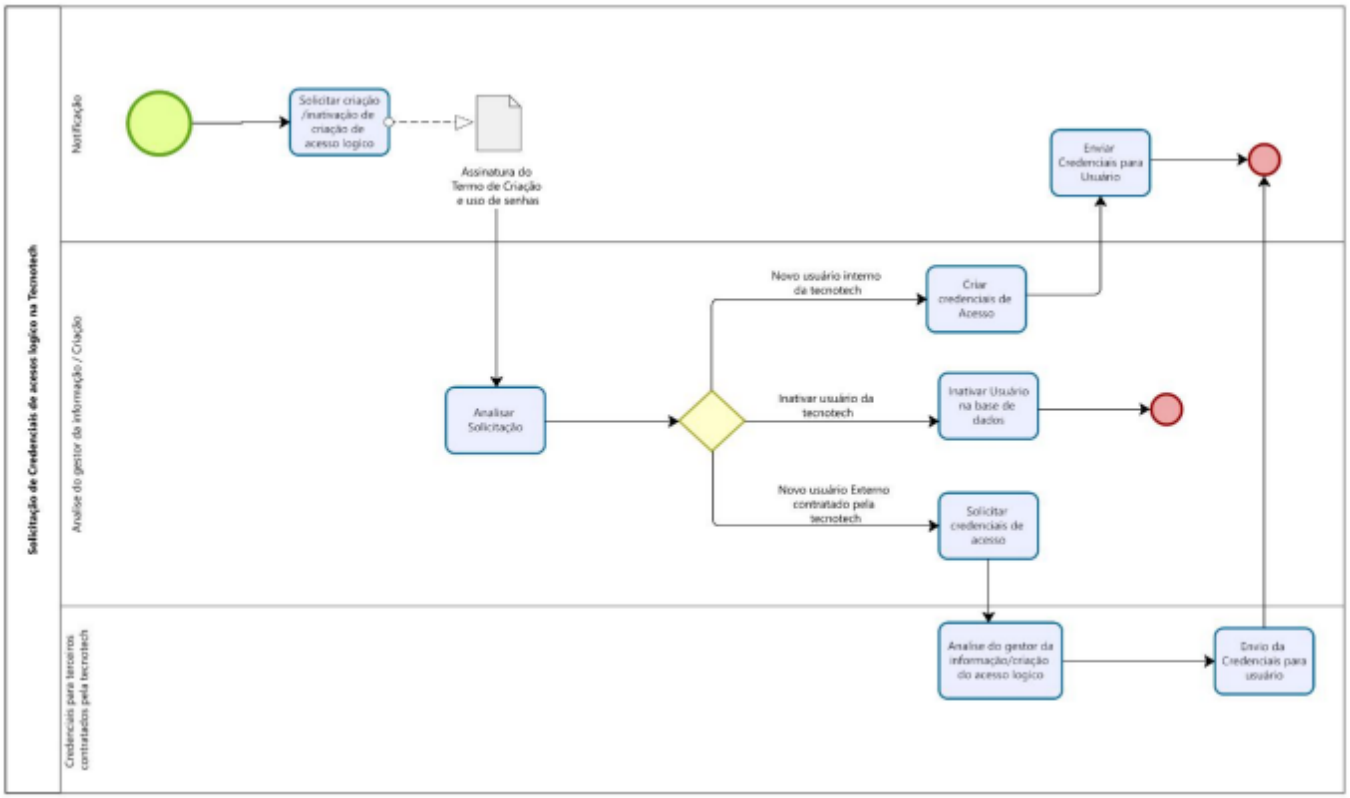

Figura 14.1: Fluxograma de acesso logico.

Capítulo 15

ANÁLISE CRÍTICA E AJUSTE DOS DIREITOS DE ACESSO DE USUÁRIO

- **Ao acesso lógico deve ser analisado criticamente e deve incluir os procedimentos.**
- **Catalogar os acessos lógicos privilegiados, bem como as modificações nestes.**
- **Garantir que o direito de acesso lógico privilegiado esteja atribuído a um identificador de usuário igual ao identificador utilizado nas atividades normais.**
- **Garantir que o direito de acesso lógico esteja em conformidade com a autorização que motivou o respectivo acesso.**

Capítulo 16

VIOLAÇÕES, PENALIDADES E SANÇÕES

- **A desobediência ou violação desta norma implicará em sanções administrativas nos termos da lei, normas complementares, regimentos e resoluções internas, sem prejuízo de outras previstas nas esferas cível e penal.**
- **Parágrafo Único: O procedimento para a aplicação das penalidades e/ou sanções seguirá o rito específico da legislação, norma, regimento ou resolução a que corresponder o caso concreto.**

Capítulo 17

DISPOSIÇÕES FINAIS

- **A elaboração e a atualização deste documento são de responsabilidade da tecnotech sistemas.**
- **Os casos omissos e as dúvidas surgidas na aplicação do disposto na Política de Controle de Acesso Lógico deverão ser analisados pela tecnotech sistemas.**
- **A presente política passa a vigorar a partir da data de sua publicação, revogando-se as disposições em contrário.**

Capítulo 18

MUDANÇAS NA POLÍTICA DE ACESSO LÓGICO

A presente versão 1.0 desta Política de controle de acesso lógico foi atualizada pela última vez em: 07/03/2023. O editor se reserva o direito de modificar, a qualquer momento as presentes normas, especialmente para adaptá-las às evoluções, seja pela disponibilização de novas funcionalidades, seja pela supressão ou modificação daquelas já existentes. Esta Política de controle de acesso lógico poderá ser atualizada em decorrência de eventual atualização normativa, razão pela qual se convida o usuário a consultar periodicamente esta seção.

Capítulo 19

CONTROLE DE VERSÕES

Tabela 19.1: Tabela de versões

Versão	Descrição	Responsável	Publicação
1.0	Versão para divulgação	Wanderson câmara - Felipe Andrade	07/03/2023

Capítulo 20

CONCORDÂNCIA

Eu li e entendi a Política de controle de acesso lógico da TECNOTECH SISTEMAS. Entendo que se eu violar as diretrizes estabelecidas nesta Política, posso enfrentar ações legais e/ou disciplinares de acordo com as leis aplicáveis e as normas internas da TECNOTECH SISTEMAS.

Assinatura do funcionário Data