CIA ESTADUAL DE ENGENHARIA DE TRANSPORTES E LOGÍSTICA CENTRAL

Código: NOR-CENTRAL-008

NP-2

Norma Interna – Gestão de Identidades e Controle de Acesso Lógico

Órgão gestor: SUPTIN	**Órgão aprovador:** DIREXE
Nº Processo: SEI-100006/001189/2024	**Data de aprovação:** 10/10/2024
Tipo:NOR - Padrão de Norma	**Versão:** 1.0
Processo: Gestão de Identidades e Controle de Acesso Lógico	**Status:** Ativo

1.OBJETIVO

Estabelecer diretrizes claras para garantir que o acesso aos ativos de informação ou sistemas da Companhia Estadual de Engenharia de Transportes e Logística – CENTRAL ofereça níveis adequados de proteção. Os controles de acesso lógicos visam proteger equipamentos, aplicativos e arquivos de dados contra perda, modificação ou divulgação não autorizada, assegurando a proteção dos dados, a integridade dos recursos tecnológicos, a segurança e a confidencialidade das informações, além de garantir conformidade com legislações e regulamentações aplicáveis.

Controles de acesso são mecanismos e políticas utilizados para gerenciar e restringir quem pode acessar recursos específicos em um si ambiente. Esses controles são essenciais para proteger informações sensíveis, garantir a privacidade e manter a integridade dos dados diferentes tipos de controles de acesso, cada um com uma função específica, entretanto, para esta norma trataremos apenas do Controle d Lógico.

O **Controle de Acesso Lógico** é o conjunto de procedimentos, recursos e meios utilizados com a finalidade de barrar ações de qualquer que possam comprometer os recursos computacionais, a rede corporativa, sistemas de informação e documentos. Podemos citar como de controle de acesso lógico as senhas para acessar os Sistemas como SEI-RJ, SIGA, etc.

2. APLICAÇÃO E ABRANGÊNCIA

Esta norma se aplica a todos os colaboradores, prestadores de serviço, estagiários, fornecedores, parceiros e qualquer pessoa que tenha acesso aos sistemas de informação, redes, serviços ou recursos tecnológicos da CENTRAL.

Todas as orientações devem ser seguidas por todos os níveis hierárquicos para assegurar a confidencialidade, integridade, disponibilidade e autenticidade das informações.

3. DOCUMENTOS DE REFERÊNCIA E COMPLEMENTARES

- Instrução Normativa PRODERJ/PRE n° 02, de 28 de abril de 2022;
- ABNT NBR ISO/IEC 27001 - Estabelece os elementos de um Sistema de Gestão de Segurança da Informação e da Comunicação;
- Controles CIS Versão 8 - Center for Internet Security® (CIS®);
- Estatuto Social da CENTRAL;
- Regimento Interno da CENTRAL;
- Política de Segurança da Informação da CENTRAL.

4. DEFINIÇÕES

Para fins de compreensão dos termos utilizados nesta política serão utilizados os seguintes conceitos e definições:

a) Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação da CENTRAL, observada eventual restrição que se aplique.

b) Ameaça: conjunto de fatores internos e externos com o potencial de causar dano para o sistema ou para a CENTRAL.

c) Alta administração: representa o mais alto nível estratégico e decisório da CENTRAL.

d) Backup/cópia de segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação.

e) Comitê de Segurança da Informação (COMISEINF): grupo de pessoas, nomeadas pela alta administração, com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito da CENTRAL.

f) Criptografia:conjunto de princípios e técnicas empregados para proteção dos dados, por meio de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno).

g) Gestor de Sistemas / da Informação: é o empregado designado comoresponsável por gerenciar e conceder acesso de um determinado sistema e/ou informações aos colaboradores (por exemplo: Gestor do SIGA, SEI-RJ, SIAFEM, e-TCE-RJ, etc.). Suas principais funções incluem controlar quem tem acesso a quais sistemas e informações dentro da empresa, assegurar que os acessos sejam seguros e restritos a pessoas autorizadas, e fornecer suporte técnico para resolver problemas de acesso e questões técnicas relacionadas.

h) Incidente: ação ou omissão que tenha permitido ou possa vir a permitir acesso não autorizado, interrupção ou mudança nas operações, destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação ou de alguma atividade por um período de tempo inferior ao tempo objetivo de recuperação.

i) Usuário: qualquer pessoa física ou jurídica que tem autorização para acessar os sistemas ou informações, redes, serviços ou recursos tecnológicos da CENTRAL, tais como funcionários, prestadores de serviço, estagiários, fornecedores e parceiros.

5. DIRETRIZES

5.1 - Ativos e sistemas de informação que devem ser protegidos

A proteção dos recursos computacionais abrange desde aplicativos e arquivos de dados até utilitários e o sistema operacional. Um invasor ou usuário não autorizado pode tentar acessar o sistema para apagar ou alterar dados, acessar aplicativos, modificar configurações do sistema operacional para facilitar futuras invasões e, posteriormente, alterar arquivos de log para ocultar suas ações. Isso pode impedir que o administrador do sistema detecte a invasão.

Os controles de acesso lógico são implementados para garantir que:

- Apenas usuários autorizados tenham acesso aos recursos.
- Os usuários tenham acesso somente aos recursos necessários para a execução de suas tarefas.
- O acesso a recursos críticos seja monitorado e restrito a um número reduzido de pessoas.
- Os usuários não possam realizar transações que não estejam alinhadas com suas funções ou responsabilidades.

O controle de acesso pode ser descrito em termos de:

- Identificação e autenticação de usuários.
- Alocação, gerenciamento e monitoramento de privilégios.
- Limitação, monitoramento e desativação de acessos.
- Prevenção de acessos não autorizados.

5.2 - Responsável pelos controles de acesso lógico

A responsabilidade pelos controles de acesso lógico pode ser atribuída tanto a SUPTIN quanto aos Gestores de Sistemas (aplicativos) e/ou de Informação. A SUPTIN controla o acesso à rede, ao sistema operacional e seus recursos, bem como os arquivos de dados, sendo responsável por proteger os recursos do sistema contra invasores ou funcionários não autorizados.

Por outro lado, os Gestores de Sistemas (aplicativos) e/ou de Informação (por exemplo: Gestor do SIGA, SEI-RJ, SIAFEM, e-TCE-RJ, etc.) são responsáveis pelo controle de acesso aos seus respectivos sistemas, identificando quem pode acessar cada um dos sistemas e quais operações podem ser executadas. Por conhecerem detalhadamente o sistema aplicativo sob sua responsabilidade, estes Gestores são as pessoas mais indicadas para definir privilégios de acesso de acordo com as reais necessidades dos usuários.

5.3 - Papéis e Responsabilidades

a) Superintendência de Tecnologia de Informação – SUPTIN:

É responsabilidade da SUPTIN, junto com a Gerência de Tecnologia da Informação - GERTIN:

- Receber e analisar solicitações para criação de contas de acesso ou fornecimento de privilégios para usuários de empregados, estagiários e terceiros/prestadores de serviços;

- Conceder, quando autorizado, o acesso aos usuários de empregados, terceiros/prestadores de serviço aos sistemas gerenciados pela SUPTIN;
- Revogar, quando solicitado, o acesso dos usuários de empregados, terceiros/prestadores de serviço aos sistemas gerenciados pela SUPTIN;
- Apoiar a revisão periódica da validade de credenciais de acesso a ativos/sistemas de informação dos usuários de empregados, terceiros/prestadores de serviço fornecendo informações sobre os privilégios atualmente efetivados em ativos/sistemas de informação.

b) Gestor do Sistema e/ou da Informação (Gestor/Ponto Focal do SIGA, SEI-RJ, SIAFEM, e-TCE-RJ, etc.)**:**

É responsabilidade dos colaboradores apontados como Gestor de Sistema e/ou da Informação:

- Autorizar a concessão e revogação de acesso a ativos/sistemas de informação sob sua responsabilidade;
- Autorizar a concessão e o controle de acesso administrativo a ativos/sistemas de informação sob sua responsabilidade;
- Realizar a revisão periódica de autorizações de acesso e credenciais de acesso a ativos/sistemas de informação sob sua responsabilidade.

c) Suprintendentes, Gerentes, Chefes de Assessoria e Equivalentes:

É responsabilidade dos gestores:

- Solicitar à SUPTIN ou ao Gestor de Sistema e/ou Informações a concessão de acesso para novos empregados ou para empregados que necessitem de novos acessos devido a mudanças em suas atividades laborais.
- Solicitar à SUPTIN ou ao Gestor de Sistema e/ou Informações a concessão de acesso a estagiários, jovens aprendizes e terceiros/prestadores de serviços contratados, justificando a necessidade de acesso a ativos/sistemas de informação.
- Informar à SUPTIN ou ao Gestor de Sistema e/ou Informações sobre o encerramento do contrato com terceiros/prestadores de serviços contratados que tenham acesso a ativos/sistemas de informação.
- Solicitar à SUPTIN ou ao Gestor de Sistema e/ou Informações a revogação das contas de acesso quando houver encerramento do contrato ou saída do empregado ou do estagiário da sua unidade.
- Reportar imediatamente qualquer incidente de segurança.

d) Superintendência de Gestão de Pessoas, Segurança e Medicina do Trabalho – SUPGEP:

É responsabilidade da SUPGEP:

- Reportar em tempo hábil o desligamento de empregados da CENTRAL a SUPTIN para que contas de acesso possam ser revogadas;
- Apoiar a gestão de identidades enviando relatórios periódicos sobre colaboradores desligados ou que mudaram de posição na CENTRAL;
- Informar a SUPTIN a criação de credenciais de acesso remoto de funcionários admitidos.
- Informar a SUPTIN a revogação de credenciais de acesso remoto de funcionários que entrarem em licenças sem vencimento, desligamento definitivo, desligamento temporário por decisão judicial, afastamentos por licença de saúde.

e) Responsáveis pela Gestão e Fiscalização dos Contratos de estagiários, terceiros/prestadores de serviço:

É responsabilidade da Gestão e Fiscalização do Contrato de estagiários, terceiros e/ou prestadores de serviço:

- Reportar em tempo hábil a SUPTIN e os Gestores de Sistemas quando do desligamento de estagiários, terceiros e/ou prestadores de serviço da CENTRAL, para que contas de acesso possam ser revogadas.

f) Comitê de Segurança da Informação – COMISEINF

- Debater e realizar revisões que tratem desta norma interna e do processo de controle de acesso.
- Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre controle de acesso.
- Propor diretrizes, competências e responsabilidades para esta norma e processo de controle de acesso.

5.4 - Gestão de Usuários

A CENTRAL fornece contas de acesso a seus usuários autorizados, permitindo o uso de ativos de informação, sistemas de informação e recursos computacionais, como a rede corporativa. Essas contas são exclusivamente para atividades laborais e para concessão de acesso aos usuários, a SUPTIN e/ou Gestores de Sistemas/Informações deverão seguir seguintes diretrizes:

a) **Criação de contas dos usuários**

- Devem ser feitas por solicitação formal e aprovação do superior hierárquico.
- O login e senha do usuário são de uso pessoal e intransferível, portanto é proibida sua divulgação ou compartilhamento, sob pena de serem bloqueados pela SUPTIN e/ou Gestor de Sistemas/ Informações quando constatada qualquer irregularidade.

b) Alteração de credenciais do usuário

- · As alterações de logins e senhas de acesso a sistemas e à rede local, quando não disponíveis nos próprios sistemas, deverão ser feitas de forma presencial pelo usuário, com a autorização da autoridade competente, junto à SUPTIN ou ao Gestor do Sistema.

c) Desativação de contas

- As contas dos usuários da CENTRAL devem ser desativadas imediatamente após o desligamento do colaborador.
- A chefia imediata será a principal responsável por monitorar e solicitar a retirada do colaborador e/ou estagiário dos sistemas, comunicando a SUPTIN e/ou o Gestor do Sistema.
- A SUPGEP será a responsável por comunicar à SUPTIN e/ou ao Gestor do Sistema do desligamento do colaborador.
- Os responsáveis pela Gestão e Fiscalização do contrato de estagiários, terceiros e/ou prestadores de serviço será o responsável por comunicar à SUPTIN e/ou ao Gestor dos Sistema do desligamento do estagiário, terceiro ou do prestador de serviço.

d) Mudança de setor e licença

- As contas dos usuários da CENTRAL devem ser desativadas imediatamente após a transferência inter setorial ou mudança de função do funcionário.
- A chefia imediata será o responsável por comunicar à SUPTIN e/ou ao Gestor do Sistema as alterações.

e) Vedada a identificação genérica e de uso compartilhado

- Não haverá identificação genérica e de uso compartilhado para acesso aos recursos da rede, excetuando-se os casos de necessidade, justificada e acompanhada de parecer da SUPTIN acerca da possibilidade de aceitação dos riscos associados.

Cada conta de acesso é pessoal e intransferível. O usuário é integralmente responsável por sua utilização e por qualquer violação ou ato irregular/ilícito realizado com sua conta, mesmo que por outra pessoa ou organização.

Os usuários devem adotar as seguintes medidas para garantir o acesso seguro aos ativos e serviços de informação:

- Não anotar ou registrar senhas de acesso em qualquer local, exceto nas ferramentas oficialmente fornecidas pela CENTRAL.
- Não utilizar sua conta, nem tentar utilizar qualquer outra conta, para violar os controles de segurança estabelecidos pela CENTRAL.
- Não compartilhar a conta de acesso e a senha com outros usuários, colaboradores ou terceiros.
- Informar imediatamente à SUPTIN qualquer falha ou vulnerabilidade que permita o acesso não autorizado a ativos de informação, sistemas ou recursos computacionais da CENTRAL.

O usuário é responsável pelo sigilo de sua senha e nos casos em que autorizar o compartilhamento de sua senha, poderá responder pelos danos causados à CENTRAL.

Qualquer utilização não autorizada ou tentativa de utilização não autorizada de credenciais e senhas será tratada como um incidente de segurança da informação, sendo sujeita à análise da infração e à aplicação de sanções e punições conforme a gravidade da violação.

5.5 - Autenticação e Autorização de acesso (privilégios de acesso)

A autorização e o nível permitido de acesso a ativos/serviços de informação da CENTRAL é feita com base em perfis que definem o nível de privilégio dos usuários.

O acesso a ativos/serviços de informação é fornecido a critério da CENTRAL, que define permissões baseadas nas necessidades laborais dos usuários edeve ser aprovada pela sua chefia imediata

Autorizações de acesso a perfis são fornecidas e/ou revogadas com base na solicitação dos gestores de cada colaborador. Solicitações deverão ser encaminhadas à equipe de tecnologia da informação.

Usuários que têm acesso autorizado a privilégios administrativos em sistemas de informação devem possuir uma credencial específica para este propósito. A credencial privilegiada deverá ser utilizada somente para a execução de atividades administrativas que requeiram esse nível de acesso, enquanto a conta de acesso comum deverá ser utilizada em atividades do dia a dia.

É expressamente proibido o armazenamento de informações de caráter pessoal, que infrinjam direitos autorais ou que não sejam de interesse da CENTRAL tanto na infraestrutura computacional local ou serviços de armazenamento remoto (nuvem).

Usuários não devem ter expectativa de privacidade quanto aos arquivos armazenados na infraestrutura computacional local ou serviços de armazenamento remoto (nuvem) da CENTRAL.

Para o controle de acesso aos funcionários de empresas contratadas e de outros órgãos conveniados, a autorização deverá ser solicitada pelo funcionário responsável direto pela requisição e pela sua Diretoria.

Os direitos de acesso aos prestadores de serviços, fornecedores e terceiros às informações e aos recursos de processamento da informação deverão ser retirados após o encerramento de suas atividades, contratos ou acordos.

Os casos omissos serão tratados pelo Diretor de Administração e Finanças.

5.6 Senha de acesso

As senhas associadas às contas de acesso a ativos/serviços de informação ou recursos computacionais da CENTRAL são de uso pessoal e intransferível, sendo dever do usuário zelar por sua guarda e sigilo.

Padrões para Geração de Senhas:

Fornecimento Inicial:

A SUPTIN ou o Gestor do Sistema ou de Informações fornecerão senhas de acesso inicial, que deverão ser trocadas imediatamente pelo usuário.

Cada sistema pode adotar uma validade ou padrão diferente para as senhas, conforme suas necessidades específicas. Entretanto, nos **Sistemas gerenciados pela CENTRAL**, a SUPTIN poderá adotar boas práticas de segurança da informação e definir a periodicidade para troca de senha do usuário.

A CENTRAL adotará seguinte padrão de senhas:

- **Comprimento da senha:** ter no mínimo de oito caracteres.
- **Caracteres numéricos:** ter no mínimo um número de 0 a 9.
- **Caracteres especiais:** ter no mínimo um caracter especial (por exemplo: !,@,#,$,%,¨,&,*).
- **Letras maiúsculas:** ter no mínimo uma letra maiúscula (A a Z).
- **Letras minúsculas:** ter no mínimo uma letra minúscula (a a z).
- A senha não deve conter o nome ou parte da conta (matrícula) do usuário ou partes do nome completo.

Histórico de Senhas:

Os sistemas manterão um histórico das últimas senhas utilizadas, não permitindo sua reutilização.

Recomendações para Criação de Nova Senha:

- Não utilizar nenhuma parte de sua credencial na composição da senha;
- Não utilizar qualquer um de seus nomes, sobrenomes, nomes de familiares, colegas de trabalho ou informação a seu respeito de fácil obtenção (ex.: placa do carro, data de aniversário, endereço);
- Não utilizar repetição ou sequência de caracteres, números ou letras;
- Não utilizar qualquer parte ou variação do nome CENTRAL;
- Evitar variações dos itens descritos acima, como duplicação ou escrita invertida.

6. REVISÕES E ALTERAÇÕES

Esta norma deve ser revisada e atualizada periodicamente pela **Superintendência de Tecnologia de Informação - SUPTIN,** ou quando houver mudanças significativas na infraestrutura ou nas regulamentações aplicáveis.

As alterações devem ser aprovadas pelo Comitê de Segurança da Informação e pela Diretoria Executiva.

SUMÁRIO DE REVISÕES		
0	10/10/2024	Emissão Original Procedimento proposto pelo Comitê de Segurança da Informação, Processo SEI-100006/001189/2024, aprovação Ata Nº 17/2024. Aprovação DIREXE em 10/10/2024 Ata Nº 347/2024.
REVISÕES	**DATA**	**DESCRIÇÃO E/OU ITENS ATINGIDOS**

-	-	-

Documento assinado eletronicamente

DIRETORIA EXECUTIVA

COMPANHIA ESTADUAL DE ENGENHARIA DE TRANSPORTES E LOGÍSTICA - CENTRAL

Distribuição: Geral

Chancela Técnica: Assessoria de Governança, Risco e Compliance - ASSGER

Rio de Janeiro, 14 outubro de 2024

Documento assinado eletronicamente por **Daiti Augusto Hamanaka**, **Assessor Chefe da ASSGER**, em 15/10/2024, às 11:31, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabricio Abilio Duarte de Moura**, **Diretor-Presidente**, em 16/10/2024, às 15:02, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **85333745** e o código CRC **B8526B1E**.

Referência: Processo nº SEI-100006/001189/2024 SEI nº 85333745

Av. Nossa Senhora de Copacabana , 493, 5º andar - Bairro Copacabana, Rio de Janeiro/RJ, CEP 22.031-000
Telefone: