Política de Segurança da Informação

Órgão aprovador: CONADM	**Data de aprovação:** 23/03/2022
Órgão gestor: ASSGER	**Versão:** 1.0
Nº Processo: SEI-100006/001246/2021	**Status:** Ativo

1 - OBJETIVO

O objetivo desta Política é servir como um instrumento de referência para a implantação de um ambiente informacional mais seguro na CENTRAL, facilitando desta forma os processos de gestão e controle.

As ações específicas para otimizar a segurança da informação deverão ser implementadas observadas as diretrizes estabelecidas nesta Política e nos normativos internos específicos e seguindo as orientações da área responsável por Segurança de Informação da Companhia.

2 - APLICAÇÃO E ABRANGÊNCIA

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, empregados e gestores ou terceiros em todos os níveis hierárquicos da Companhia de Engenharia de Transportes e Logística – CENTRAL.

A política é aplicável tanto ao ambiente informatizado quanto aos meios convencionais de processamento, comunicação e armazenamento da informação. Abrange todos os equipamentos utilizados pela CENTRAL, próprios ou contratados de terceiros.

3 -DOCUMENTOS DE REFERÊNCIA E COMPLEMENTARES

- Constituição Federal de 1988;
- Lei Nº 12.527/2011 - Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal;
- Lei nº 13.709/2018 - Lei Geral de Proteção de Dados (LGPD);

- Decreto nº 9.637/2018 - Instituiu a Política Nacional de Segurança da Informação
- Estatuto Social da CENTRAL;
- Norma ABNT NBR/ISO/IEC 27001:2013 - Estabelece os elementos de um Sistema de Gestão de Segurança da Informação e da Comunicação.

4 - DEFINIÇÕES

A segurança da informação visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela instituição. A integridade, a confidencialidade e a autenticidade de informações estão intimamente relacionadas aos controles de acesso.

4.1 Termos e Definições:

Ativos de Informação: os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e os recursos humanos que a eles têm acesso;

Ambiente Informatizado: agregado de indivíduos, organizações e/ou sistemas que coletam, processam ou disseminam informação;

Análise de Risco de Vulnerabilidades: avaliação das ameaças, impactos e vulnerabilidades;

Confidencialidade de informações: consiste na garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas (em meios físicos ou digitais) ou transmitidas por meio de redes de comunicação. Manter a confidencialidade pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento;

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;

Disponibilidade de informações: consiste na garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática, quando se tratar de meios digitais. Manter a disponibilidade de informações pressupõe garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem é de direito;

Integridade de informações: consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados, em meios físicos ou digitais, com relação às inserções, alterações e processamentos autorizados efetuados. Sinaliza, ainda, a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário. A manutenção da integridade pressupõe a garantia de não violação dos dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital;

Política de segurança da informação: documento aprovado pela autoridade responsável pelo órgão com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da Segurança de Informação;

Segregação de Funções: princípio básico de controle interno essencial para a sua efetividade. Consiste na separação de atribuições ou responsabilidades entre diferentes pessoas, especialmente as funções ou atividades-chave de autorização, execução, atesto/aprovação, registro e revisão.

5 - AUTORIDADE E RESPONSABILIDADES

A responsabilidade quanto à segurança da informação é de todos os empregados, colaboradores e gestores da CENTRAL, e deve ser amplamente divulgada.

É de responsabilidade de todos os empregados/colaboradores/gestores cuidar da integridade, confidencialidade e disponibilidade dos ativos de informação da CENTRAL, devendo ser comunicadas quaisquer irregularidades, falhas ou desvios identificados à sua chefia imediata, assim como a área responsável pela segurança da informação.

Esta Política de Segurança compromete e responsabiliza cada colaborador, empregado e gestor, dando ciência que a CENTRAL, conforme previsto nas leis brasileiras mantém os ambientes, telefones, sistemas, computadores e redes da

empresa sujeita a monitoramento e gravação, buscando assegurar a correta utilização dos recursos por ela oferecidos a seus colaboradores.

Exceções a esta política deverão ter seus pleitos formalizados ao Comitê de Segurança da Informação onde serão deliberados e, caso assim sejam julgados, aprovados em caráter excepcional (aprovação por exceção).

Até a instituição do Comitê de Segurança da Informação na Companhia, as exceções a esta política, serão julgadas e aprovadas pelo Diretor de Administração de Finanças – DIRAF.

O Comitê de Segurança da Informação deverá ser composto por um (01) membro representante de cada Diretoria, sendo obrigatória a participação de um (01) membro representante da área de TI e um (01) membro representante da área de Governança, designados por Portaria do Diretor-Presidente da CENTRAL.

O Comitê de Segurança da Informação a ser instituído na Companhia terá como objetivos:

a) Promover cultura de Segurança da Informação;
b) Propor normas internas e procedimentos relacionados à Segurança da Informação;
c) Propor recursos necessários às ações de Segurança da Informação;
d) Coordenar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, caso a CENTRAL adote;
e) Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na Segurança da Informação;
f) Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança da informação;
g) Dar suporte necessário à gestão da Política de Segurança da Informação.

O Comitê se reunirá ordinariamente, em periodicidade mensal, com o objetivo de acompanhar o andamento das ações relativas à segurança, e extraordinariamente, por solicitação de qualquer de seus membros para tratar de assuntos pontuais.

A revisão deste documento deve ser executada pelo Comitê de Segurança da Informação anualmente, ou quando necessário.

6 - DIRETRIZES

6.1 Recomendações para Gestão dos Ativos de Informação

Toda e qualquer informação gerada, adquirida, utilizada ou armazenada é considerada de sua propriedade da CENTRAL e deve ser protegida.

Toda a informação deve ter um responsável pela sua criação, aquisição, manutenção, atualização e segurança.

A Política de Segurança da Informação, bem como o seu cumprimento, deve ser objeto de auditorias periódicas realizadas pela Auditoria Interna.

Os ativos de informação devem ser protegidos contra ações indevidas intencionais ou acidentais que impliquem perda, destruição, inserção, cópia, extração, alteração, uso e exposição indevidos, em conformidade com os princípios da confidencialidade, integridade e disponibilidade.

Os ativos de informação devem ser mantidos com o mesmo nível de proteção, independente do meio no qual estejam armazenados, em que trafeguem, ou ainda do ambiente em que estejam sendo processados.

Mecanismos de prevenção, detecção, e eliminação de vírus de computador e de outros programas maliciosos devem ser utilizados de forma preventiva e reativa.

Os colaboradores, empregados e gestores, devem declarar o seu conhecimento e comprometimento com a Política de Segurança da Informação, através da assinatura de um TERMO DE SIGILO, CONFIDENCIALIDADE E NÃO DIVULGAÇÃO.

6.2 Recomendações para Gestão de Ativos Físicos

Todos os ativos devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos.

Todos os usuários devem estar cientes de suas responsabilidades para a manutenção efetiva dos controles de acesso, considerando o uso e a confidencialidade de suas senhas e a segurança de seus equipamentos.

Ao utilizar equipamentos de computação móveis (notebooks, computadores de mão, telefones celulares, etc.), os usuários devem ter cuidados especiais a fim de garantir que as informações da Companhia não sejam comprometidas.

6.3 Recomendações para controle de acesso

As regras de controle de acesso a todo sistema corporativo, Intranet, internet, informações, dados, documentos físicos e às instalações físicas deverão ser definidas e regulamentadas, através de Normas Internas (NIs), com o objetivo de garantir a segurança dos usuários e a proteção dos ativos.

A senha de acesso de cada empregado/colaborador utilizada como assinatura eletrônica deverá ser mantida secreta, vetado o seu compartilhamento.

A identificação de acesso (usuário de rede) deverá ser única, pessoal e intransferível, não devendo ser utilizado login genérico, salvo em casos a serem aprovados pela Assessoria de Tecnologia da Informação.

As permissões de acesso devem ser concedidas de acordo com as atribuições dos usuários, sempre por necessidade de trabalho.

O acesso ao ativo da informação não gera direito real sobre o mesmo e nem sobre os frutos de sua utilização.

Todos os acessos devem ser rastreáveis para que o usuário seja identificado individualmente.

6.4 Recomendações para Gestão de Riscos

As medidas de segurança devem ser adotadas de forma proporcional aos riscos existentes e a magnitude dos potenciais danos, considerando o ambiente, o valor e a criticidade da informação.

6.5 Recomendações para Treinamento em Segurança da Informação

Os colaboradores devem ser treinados e capacitados a exercerem as atividades inerentes ao objeto da Companhia com a visão de segurança da informação.

6.6 Recomendações para Alinhamento das Áreas Fins e Tecnologia

As iniciativas e projetos das áreas de negócio e tecnologia devem estar alinhados com as diretrizes e arquiteturas de segurança da informação, garantindo a confidencialidade, integridade e disponibilidade das informações.

6.7 Recomendações para Segurança Física do Ambiente

O processo de segurança física deve estabelecer controles de acesso somente às pessoas autorizadas, de acordo com a criticidade das informações previamente mapeadas, devendo ser igualmente respeitadas às normas de segurança de acesso definidas pela Administração Predial.

6.8 Recomendação para Utilização do Correio Eletrônico Corporativo

É obrigatório o uso de endereço eletrônico institucional para recebimentos, envios ou quaisquer meios análogos de prestação laboral à CENTRAL.

O colaborador deve utilizar e divulgar seu endereço de e-mail corporativo exclusivamente para mensagens relacionadas às suas atividades na Companhia, não devendo em hipótese alguma, utilizá-lo para cadastros em sites de compras, relacionamentos, dentre outros.

Deve ser vedado o envio de informações críticas para pessoas ou organizações não autorizadas, observando, quando for o caso, orientações para o tratamento de informações classificadas.

É ainda vedado o envio de material obsceno, ilegal ou não ético, envio de propaganda, mensagens do tipo corrente e de entretenimento, e ainda mensagens relacionadas à nacionalidade, raça, orientação sexual, orientação religiosa, convicção política ou qualquer outro assunto que possa vir a configurar difamação ou discriminação e que não tenha relação com o serviço ao qual o usuário é destinado no ambiente de TI ou qualquer outro ambiente da CENTRAL.

É vedada também a participação em Listas de Discussão, utilizando o serviço de Correio Eletrônico Corporativo, que possam abordar assuntos alheios às atividades da CENTRAL, suas diretorias e suas gerências, exceto em casos de participação em

Listas de Discussão sobre assuntos relacionados às atividades desenvolvidas na Companhia.

Por se tratar de uma ferramenta de trabalho, as mensagens recebidas e/ou enviadas pelo profissional podem ser auditadas sem necessidade de conhecimento e/ou autorização prévia e, havendo constatação de uso inadequado poderão ser apagados de forma definitiva.

6.9 Recomendação para a Utilização dos Recursos de Armazenamento de Dados em Nuvens Computacionais

A utilização de ferramenta para armazenamento na nuvem não homologada pela CENTRAL deve ser justificada e autorizada pelo superior do solicitante.

Devem ser definidos na norma específica os dados que podem ser transitados através da nuvem e os cuidados a serem adotados, a responsabilidade pelo vazamento de informação e proibição de armazenagem de determinados arquivos.

A norma também deverá prever os mecanismos a serem adotados após fim do contrato profissional, o qual todos os acessos serão revogados e é necessário que o líder/superior do profissional solicite para a área de TI o backup dos dados, pois com a exclusão da conta do profissional o conteúdo online poderá ser perdido.

6.10 Recomendação para a Utilização de Dispositivos e Equipamentos Particulares BYOD – “Bring Your Own Device” na CENTRAL

Deverá ser objeto de regulamentação interna a utilização de dispositivos e equipamentos particulares no ambiente corporativo pelos funcionários.

A norma específica para prática do BYOD deverá conter diversas medidas de segurança como orientações para utilização de acessos ao equipamento com senha, instruções para encriptar as informações gravadas na memória do equipamento do usuário, mecanismo de controle de acesso às informações pertinentes à empresa, estabelecimento das tecnologias obrigatórias de segurança, esclarecimento minucioso das responsabilidades/penalidades, limite/hierarquização de acessos e entre outros.

6.11 Recomendações para Recuperação de Dados

Deverão ser providos recursos para a geração de cópias de segurança e de recuperação de informações, devidamente documentadas, abrangendo periodicidade de cópias, forma e local de armazenamento, autorização de uso, prazo de retenção e plano de simulação e testes.

6.12 Recomendações para Auditoria

Deverão ser providos recursos para o registro de informações do tipo trilha de auditoria com prazos de retenção e formas de acesso definidas, com vistas a permitir auditoria, identificação de situações de violação e contabilização individual do uso dos sistemas.

6.13 Recomendações para Segurança do Ambiente Computacional

No ambiente informatizado da CENTRAL, devem ser utilizados e instalados somente softwares homologados e originais.

Os softwares instalados nos equipamentos servidores, nos equipamentos de rede e comunicação, nas estações de trabalho e nas mesas de trabalho devem ser permanentemente atualizados, visando incrementar aspectos de segurança e correção de falhas.

A eliminação da informação protegida por sigilo fiscal, ou de uso exclusivo da CENTRAL e de softwares instalados, constantes em dispositivos de armazenamento, deve ser precedida da utilização de ferramentas adequadas à eliminação segura dos dados.

Devem ser adotadas medidas adicionais de proteção, visando garantir o mesmo nível de segurança das instalações internas da CENTRAL no caso de:

a) Uso de computação móvel, dispositivos móveis, mídias removíveis e quando o usuário utilizar o seu próprio equipamento (este último quando sua utilização for expressamente autorizada);
b) Uso de acesso remoto ou de rede instalada em ambiente informatizado diferente da CENTRAL, e;
c) Comunicação sem fio.

O tráfego de informações em redes locais e de longa distância deve ser protegido contra danos, perdas, indisponibilidades, uso ou exposição indevida, de acordo com seu valor, criticidade e confidencialidade.

As redes de dados devem possuir, sempre que possíveis rotas alternativas, além de contar com mecanismos de redundância.

6.14 Recomendações para aplicação de penalidades

O descumprimento das disposições constantes nesta Política e demais diretrizes de segurança da informação caracterizará infração funcional.

Ações que violem a Política de Segurança da Informação, diretrizes, normas e procedimentos, ou que afetem ou prejudiquem os controles serão passíveis de investigação, podendo implicar em penas e sanções legais impostas por meio de medidas administrativas, sem prejuízo das demais medidas cíveis e penais cabíveis.

7 - REGISTROS

Não aplicável.

8 -ANEXOS

Não aplicável.

Sumário de Revisões		
0	23/03/2022	Emissão Original. Política proposta pela ASSGER em conjunto com a DIRAF, processo SEI-100006/001246/2021. Aprovação ASSJUR em 17/11/2021 (24934380). Validação DIREX em 25/02/22, Ata Nº 308. Aprovação CONADM em 23/03/22, Ata Nº 208.
Revisões:	**Data:**	**Descrição E/Ou Itens Atingidos**