1. OBJETIVO

1.1. Esta Norma regulamenta e estabelece as diretrizes de uso responsável da ***internet***, por meio de **recursos tecnológicos** cedidos para fins de trabalho e tem como objetivo disseminar as regras de utilização desse serviço de forma a preservar a confidencialidade, integridade e disponibilidade das **informações**.

2. ABRANGÊNCIA

2.1. Esta Norma aplica-se a todos os **colaboradores**, **gestores**, **diretores, presidente-executivo,** representante de órgãos de governança corporativa, terceiro ou qualquer **parte interessada** ou **relacionada** que necessite acessar a *internet* para fins de trabalho ou estabelecimento de relação profissional com o grupo societário da Federação das Empresas de Mobilidade do Estado do Rio de Janeiro (Semove). Para esta finalidade, esses indivíduos serão denominados **usuários** de recurso tecnológico para fins de interpretação desta Norma.

2.2. O nível de classificação da informação desta Norma é público.

2.3. O usuário deve ser categorizado como “usuário interno” quando a credencial de acesso aos recursos tecnológicos tem domínio “@semove.org.br”. Caso contrário, deve ser categorizado como “usuário externo”.

2.4. Todas as palavras ou expressões destacadas em **negrito** estão definidas no Glossário (ANEXO III).

2.5. As diretrizes desta Norma não se sobrepõem à legislação ou a convenções coletivas de trabalho em vigor e se complementam às definições previstas no contrato social,

regimentos internos ou instrumentos normativos que tenham sido divulgados pela Semove.

3. REFERÊNCIA LEGAL E BOAS PRÁTICAS

- ABNT NBR ISO/IEC 27001:2013 - Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão da Segurança da Informação - Requisitos.
- Código de Conduta.
- Constituição da República Federativa do Brasil/1988.
- Contrato Social da Semove.
- Decreto-Lei nº 2.848/1940 - Código Penal Brasileiro.
- Decreto-Lei nº 5.452/1943 - Consolidação das Leis do Trabalho (CLT).
- Decreto-Lei nº 11.491/2023 - Promulga a Convenção sobre o **Crime Cibernético**, firmada pela República Federativa do Brasil.
- Lei nº 10.406/2002 - Código Civil.
- Lei nº 12.737/2012 - Dispõe sobre a tipificação criminal de delitos informáticos.
- Lei nº 12.965/2014 - Marco Civil da *Internet*.
- Lei nº 13.709/2018 - Lei Geral de Proteção de Dados (LGPD).
- Lei nº 14.155/2021 - Dispõe sobre a gravidade dos crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela *internet*.
- Norma de Boas Práticas em Redes Sociais e Demais Ambientes Digitais.
- Norma de Gestão de Criptografia e Gerenciamento de Chaves Criptográficas.
- Norma de Gestão dos Registros de Auditoria (*logs* de auditoria).
- Política de Consequências.
- Política de Proteção de Dados e Privacidade (PLGPD).

- Política de Segurança da Informação (PSI).
- Política do Canal de Denúncia e Diálogo Voz Ativa.
- Regimento Interno do **Comitê de Integridade e Conformidade (CIC).**

4. VIGÊNCIA

4.1. Esta Norma entra em vigor a partir da data de sua publicação. A revisão deverá ser realizada em até 3 (três) anos, contados da data de sua efetiva publicação, ou sempre que a Gerência de Segurança da Informação julgar necessário.

4.2. Não obstante, ainda que não tenha sido renovada, suas diretrizes permanecem válidas até a publicação da próxima versão.

5. RESPONSABILIDADES

5.1. Todos devem cumprir as diretrizes desta Norma, legislação vigente e demais instrumentos normativos correlatos, bem como suas respectivas atualizações, de modo a evitar a ocorrência de **incidentes de segurança da informação**, que podem causar danos significativos à Semove, prejudicando a sua marca, reputação ou operação/negócio no mercado em que atua. No entanto, algumas funções, áreas ou órgãos de governança têm atribuições/responsabilidades adicionais perante suas diretrizes, tais como:

i. ***Comitê de Integridade e Conformidade (CIC)****:* seus representantes devem i) tomar ciência, revisar e apoiar a disseminação desta Norma; e ii) em caso de denúncia, recomendar, quando cabível, a aplicação de medidas disciplinares ao colaborador, gestor e **agente de governança**, quando comprovada sua culpa ou

dolo, em ações que resultem no descumprimento desta Norma ou configurem violações à legislação em vigor.

ii. ***Conselho de Gestão (CG)****:* seus conselheiros devem: i) deliberar sobre a aplicação de medidas disciplinares ao diretor ou presidente-executivo, quando comprovado que este tenha, direta ou indiretamente, contribuído para a ocorrência ou tenha se envolvido em violações à legislação em vigor ou às diretrizes desta Norma ou demais instrumentos normativos; e ii) aprovar esta Norma, de modo que seja possível a divulgação nos canais de comunicação da Semove.

iii. *Diretoria Jurídica/Coordenação Jurídica*: é área subordinada à Diretoria Jurídica, responsável por: i) prover apoio legal e consultivo ao **Órgão Diretivo** na condução dos negócios, ii) apoiar o Órgão Diretivo, na avaliação e definição de sanção, medida disciplinar ou, em última instância, ajuizamento de ação de responsabilização administrativa, civil ou penal aplicável ao infrator, quando cabível, por ato praticado em desacordo com a legislação vigente ou instrumentos normativos publicados, em especial quando decorrerem de incidentes de segurança da informação provocados por mau uso da *internet* para fins de trabalho; iii) revisar esta Norma; e iv) solicitar, quando requerido, a credencial de acesso aos recursos tecnológicos corporativos para conselheiros do CG ou delegados da AGRS da Semove.

iv. *Gerência de Auditoria Interna*: deve: i) assessorar a alta administração, o CIC e/ou demais órgãos fiscalizadores, quando instituídos, na identificação e no monitoramento dos riscos, bem como na fiscalização, investigação e tratamento de atos ilícitos e/ou em desacordo com esta Norma ou demais instrumentos normativos, principalmente quando se tratar de incidentes de segurança da

informação significativos, visando, de forma independente e imparcial, apoiar os gestores e o Órgão Diretivo no aprimoramento dos processos das áreas de negócios sob sua estrutura organizacional; e ii) opinar e comunicar à alta administração, quando cabível, as não conformidades identificadas por meio do acompanhamento dos planos de ações decorrente de auditorias, do CIC ou de investigações realizadas, visando engajar o Órgão Diretivo no adequado gerenciamento de riscos e, consequentemente, na busca pela melhoria contínua nos processos sob sua estrutura organizacional.

v. *Gerência de Comunicação Institucional*: deve divulgar esta Norma nos canais de comunicação da Semove.

vi. *Gerência de Controles Internos e Riscos*: é responsável por: i) assessorar as áreas de negócios na detecção, prevenção e remediação de riscos decorrentes de vulnerabilidades identificadas nos processos e controles das áreas de negócios que, pela diretriz desta Norma, possam acarretar incidentes de segurança da informação; ii) revisar e submeter esta Norma às instâncias aprovadoras competentes; iii) apoiar, quando requerido e em caráter consultivo, a Gerência de Auditoria Interna ou demais áreas responsáveis por procedimentos de auditoria, fiscalização e investigação de atos suspeitos ou confirmados, que sujeitem a Semove a incidentes de segurança da informação significativos, em diligências ou investigações internas de condutas que indiquem o descumprimento das diretrizes desta Norma, ou que configurem violações à legislação em vigor; e iv) solicitar, quando requerido, a credencial de acesso aos recursos tecnológicos corporativos para os representantes do CIC.

vii. *Gerência de Desenvolvimento Organizacional*: deve: i) apoiar a Gerência de Segurança da Informação nos treinamentos que tratem da conscientização

quanto às diretrizes desta Norma; e ii) solicitar a credencial de acesso para recursos tecnológicos corporativos aos usuários internos no momento da admissão.

viii. *Gerência de Infraestrutura/Coordenação de Service Desk*: é a área técnica subordinada à Gerência de Infraestrutura, responsável por: i) efetuar as configurações nos recursos tecnológicos e promover a infraestrutura necessária aos usuários para acesso à *internet*; ii) homologar e analisar o licenciamento de ***softwares***, sistemas e aplicativos; iii) apoiar a Gerência de Segurança da Informação na análise e remediação de vulnerabilidades decorrentes de acesso a *websites* ou instalação de *softwares*, sistemas ou aplicativos nos recursos tecnológicos **corporativos**, frente aos padrões de segurança da informação; iv) solucionar os chamados registrados na Central de Serviços pelos usuários internos acerca da indisponibilidade ou mau funcionamento da *internet* e dos recursos tecnológicos corporativos; v) apoiar a Gerência de Segurança da Informação na definição das soluções tecnológicas que visem proteger as informações armazenadas nos recursos tecnológicos corporativos contra incidentes de segurança da informação, principalmente os crimes cibernéticos; vi) revisar esta Norma; e vii) guardar os **Termos de Recebimento e Uso** e os **Termos de Devolução** dos *notebooks*, computadores, monitores e demais recursos tecnológicos cedidos pela Semove que estão sob sua gestão.

ix. *Gerência de Proteção de Dados e Privacidade*: é responsável por: i) avaliar os processos das áreas de negócios que tratem **dados pessoais** (**sensíveis** ou não), de forma a definir e recomendar a implementação de controles que mitiguem a ocorrência de incidentes de segurança da informação, envolvendo vazamento de dados pessoais (sensíveis ou não); ii) prover apoio acerca da proteção e

privacidade dos dados pessoais (sensíveis ou não); iii) apoiar a Gerência de Auditoria Interna ou demais áreas responsáveis por procedimentos de auditoria, fiscalização ou investigação de atos, suspeitos ou confirmados, que sujeitem a Semove a incidentes de segurança da informação de impacto significativo, por exposição de dados pessoais; iv) liderar os requerimentos e relacionamentos com entes fiscalizadores da LGPD; e v) revisar esta Norma.

x. *Gerência de Relações do Trabalho*: é responsável por solicitar a revogação da credencial de acesso do usuário interno aos recursos tecnológicos corporativos, quando houver desligamento ou afastamento legal.

xi. *Gerência de Segurança da Informação*: é a área técnica responsável por: i) conceder, suspender, revogar, restringir e monitorar o acesso à *internet* por meio de utilização de recurso tecnológico corporativo, para fins de trabalho; ii) homologar a aderência dos **navegadores**, *website*, *softwares*, sistemas e aplicativos aos padrões de segurança e privacidade da **informação** estabelecidos pela Semove; iii) detectar, prevenir e remediar a ocorrência de incidentes de segurança da informação; iv) apoiar tecnicamente a Gerência de Auditoria Interna na tratativa de denúncias envolvendo incidentes de segurança da informação; v) remediar os incidentes de segurança da informação de baixo ou médio impacto, com o apoio das áreas técnicas competentes; vi) solicitar a instauração de um **Grupo de Gestão de Incidentes de Segurança da Informação**, em caso de ocorrência de incidentes de segurança da informação de impacto significativo para a Semove, assumindo o compromisso de envolver a Gerência de Auditoria Interna no acompanhamento das tratativas realizadas pelas áreas técnicas e/ou a Gerência de Proteção de Dados e Privacidade, quando houver vazamento de dados pessoais; vii) revisar esta Norma; viii) coletar as assinaturas

eletrônicas e realizar a gestão dos Termos de Aceite desta Norma (ANEXO I), assegurando a guarda segura e a disseminação de suas diretrizes aos usuários internos.

xii. realizar a gestão dos Termos de Aceite desta Norma (ANEXO I), zelando para que os usuários internos a conheçam e adiram às suas diretrizes.

xiii. *Gestores:* responsáveis por: i) conhecer, cumprir e assegurar que seus colaboradores e/ou terceiros sob sua gestão ajam em conformidade com a legislação, convenções, regimentos internos, diretrizes desta Norma e demais instrumentos normativos ou contratuais; ii) apoiar, executar ou cobrar a execução de plano de ação que possa ter sido definido para si ou para seus colaboradores e/ou terceiros, com o intuito de mitigar o risco de ocorrência de incidentes de segurança da informação; iii) aplicar medidas disciplinares ou requerer à Diretoria Jurídica/Coordenação Jurídica, o ajuizamento de ação de responsabilização administrativa, civil ou penal, ao colaborador e/ou terceiro que esteja sob sua estrutura organizacional, quando comprovado que este tenha, direta ou indiretamente, contribuído para a ocorrência ou tenha se envolvido em violações à legislação em vigor ou às diretrizes desta Norma e demais instrumentos normativos vigentes; iv) aplicar, desde que autorizado, sanção contratual à pessoa jurídica contratada pela Semove, quando comprovada a culpabilidade do seu prestador de serviço em alguma infração que resulte em incidentes de segurança da informação; e vii) solicitar e realizar a gestão dos Termos de Aceite desta Norma (ANEXO II), zelando para que os usuários externos (ex.: fornecedores, clientes, parceiros ou demais partes interessadas) sob sua gestão contratual a conheçam e adiram às suas diretrizes, caso façam uso da *internet* durante seu relacionamento com a Semove.

xiv. *Grupo de Gestão de Incidentes de Segurança da Informação:* i) definir e submeter à alta administração um plano de ação estratégico que vise remediar a crise gerada por **incidente de segurança da informação** de impacto significativo, até que haja o restabelecimento do estado de normalidade dos negócios da Semove em seu mercado de atuação, principalmente preservando e restabelecendo seus relacionamentos com suas partes interessadas ou relacionadas; ii) comunicar o plano de ação e o prazo de execução às equipes atuantes na manutenção da operação ou negócio-chave da Semove; iii) monitorar o cumprimento do plano de ação determinado pela equipe estratégica; e iv) comunicar o *status* de execução do plano de ação, na periodicidade acordada, à alta administração e, quando autorizado, às suas partes interessadas ou relacionadas.

xv. *Órgão Diretivo*: responsável por: i) conhecer, cumprir e assegurar que seus gestores e colaboradores ajam em conformidade com a legislação, convenções, regimentos internos ou diretrizes desta Norma e demais instrumentos normativos ou contratuais; ii) apoiar, executar ou cobrar a execução de plano de ação que possa ter sido definido para si ou para seus subordinados, com o intuito de mitigar o risco de ocorrência de incidentes de segurança da informação, enquanto navegam na *internet*; iii) deliberar sobre o apetite e tolerância ao risco que impactam as áreas de negócios sob suas respectivas lideranças; iv) aplicar medidas disciplinares, ou requerer à Diretoria Jurídica/Coordenação Jurídica, o ajuizamento de ação de responsabilização administrativa, civil ou penal, ao gestor que esteja sob sua estrutura organizacional, quando comprovado que este tenha, direta ou indiretamente, contribuído para a ocorrência, ou tenha se envolvido em violações à legislação em vigor ou às diretrizes desta Norma e demais instrumentos normativos vigentes; v) deliberar sobre a aplicação de

sanção contratual à pessoa jurídica contratada pela Semove, quando comprovada a culpabilidade do seu prestador de serviço em alguma infração que resulte em incidentes de segurança da informação; vi) definir os profissionais que irão compor o Grupo de Gestão de Incidentes de Segurança da Informação, em caso de ocorrência de incidente de segurança da informação de impacto significativo para a Semove; e vii) deliberar sobre ações emergenciais recomendadas pelo Grupo de Gestão de Incidentes de Segurança da Informação, em eventual crise.

xvi. *Supervisão Administrativa e de Manutenção*: é responsável por: i) definir, junto com a Gerência de Infraestrutura/Coordenação de *Service Desk,* os requisitos técnicos minimamente necessários para assegurar o adequado funcionamento dos aparelhos celulares corporativos para fins de trabalho; e ii) guardar os Termos de Recebimento e Uso e os Termos de Devolução dos aparelhos celulares e demais recursos tecnológicos cedidos pela Semove que estejam sob sua gestão.

6. DIRETRIZES GERAIS

6.1. As regras previstas nesta Norma visam ao desenvolvimento de um comportamento eminentemente íntegro, diligente e seguro pelo usuário ao acessar a *internet* no exercício de suas funções.

6.2. O acesso à *internet* no trabalho deve ocorrer por meio de recursos tecnológicos fornecidos pela Semove, tais como: computadores, *notebooks*, aparelhos celulares e demais **dispositivos móveis**.

6.3. A *internet* disponibilizada pela Semove deve ser usada exclusivamente para fins profissionais ou laborais. O uso da *internet* deve estar amparado por ferramentas de segurança da informação, homologadas pelas áreas técnicas da Gerência de Infraestrutura/Coordenação de *Service Desk* e Gerência de Segurança da Informação. Essas ferramentas devem estar atualizadas para a última versão sistêmica liberada pelo fabricante, de modo que seja possível detectar, prevenir e remediar, com determinada eficiência, possíveis incidentes de segurança da informação.

6.4. A PSI proíbe o uso de **ativos** corporativos para fins privados com o objetivo de reduzir a exposição de suas informações a terceiros não autorizados. O conteúdo acessado na *internet*, seja por meio de rede privada ou corporativa, pode acarretar exposição indevida de informações corporativas, seja por falha do próprio usuário ao desrespeitar as boas práticas de segurança da informação, seja por vulnerabilidades de segurança da informação.

6.5. O acesso à *internet* dentro das dependências da Semove ocorre por meio de rede *wi-fi* ou cabeada e será concedido aos colaboradores, gestores, agentes de governança ou terceiros, se autorizados. É proibida a concessão de acesso à *internet* a conhecidos, **parentes**, **aparentados por afinidade**, que, porventura, visitem as dependências da Semove, ainda que em caráter temporário, se este acesso for dispensável aos interesses da Semove.

6.6. Sempre que o usuário estiver fora das dependências da Semove, deverá obrigatoriamente acessar a *internet* por meio de **rede privada virtual** (***Virtual Private Network*** ou ***VPN***) disponibilizada pela Semove, pois é o que assegura a criptografia e proteção dos dados trafegados.

6.7. É proibido o acesso às informações corporativas por meio de *internet* provida em locais públicos (i.e., praia, praça, lojas, *shoppings*, aeroporto etc.), uma vez que não são seguras e podem ser utilizadas por atacantes para monitorar o tráfego de dados. Nesses casos, recomenda-se o uso do aparelho celular corporativo para consultar as informações ou para rotear o acesso ao recurso tecnológico.

6.8. O usuário interno que, pelo cargo que ocupe (ex.: gestores, diretores, presidente-executivo) ou função que exerça no trabalho, faça jus à utilização de aparelho celular corporativo (ex.: colaboradores que realizem trabalhos externos, lidem com informações confidenciais ou que contemplem dados pessoais) deve acessar a *internet* via *wi-fi* corporativa ou, quando autorizado, via *chip* de dados móveis das linhas telefônicas contratado e disponibilizado pela Semove.

6.9. Na hipótese de uso de *internet* provida por terceiros (ex.: fornecedores, parceiros comerciais, hotéis, *home office* etc.), caberá ao usuário interno acessá-la por meio de *VPN* corporativa, além de observar e cumprir as políticas de segurança e privacidade das informações vigentes no ambiente terceirizado, sem prejuízo das orientações previstas nesta Norma, PSI ou demais instrumentos normativos.

6.10. Com a evolução tecnológica, os incidentes de segurança da informação têm impactado as organizações, comprometendo seus negócios, marca e reputação. Tanto o usuário envolvido quanto a própria pessoa jurídica poderão responder pelas ações praticadas pelo mau uso da *internet*, capazes de acarretar danos a si próprio, a terceiros ou ao próprio negócio da Semove. Dependendo da infração e seu impacto, tanto a Semove quanto o Órgão Diretivo podem: envolver-se em litígios de responsabilização individual ou coletiva; sujeitar-se às sanções contratuais ou legais; serem obrigados a reportar o incidente de segurança da informação aos titulares de dados pessoais, aos órgãos fiscalizadores, às auditorias

e à sociedade; interromper ou encerrar suas atividades, dentre outras consequências.

6.11. A Semove deve treinar seus usuários periodicamente, de modo que utilizem os recursos tecnológicos corporativos de forma segura, ao acessar a *internet*, provendo orientações e treinamentos sobre segurança e privacidade da informação (incluindo o uso de inteligência artificial).

6.12. O vazamento intencional de informações corporativas é uma infração prevista na Política de Consequências passível de demissão, podendo o autor responder por crime e ressarcimento do prejuízo financeiro sofrido em decorrência deste compartilhamento não autorizado, portanto, é importante que o usuário da *internet* tenha cautela ao lidar com informações confidenciais (i.e., internas, restritas ou sigilosas), ou até mesmo aquelas classificadas como públicas, quando ainda não tiver sido autorizada a sua publicação pelo Órgão Diretivo. O vazamento de informações permite que terceiros acessem, de forma privilegiada, informações acerca das diretrizes estratégicas, projetos, campanhas e ações operacionais e táticas da Semove e as utilizem inadequadamente.

7. CONCESSÃO E REVOGAÇÃO DE ACESSO À *INTERNET*

7.1. Por ocasião da admissão, a Gerência de Desenvolvimento Organizacional solicita a credencial de acesso, mediante abertura de chamado na Central de Serviços, para o colaborador, gestor, diretor, presidente-executivo, que, na qualidade de usuário interno, necessite dessa credencial para o exercício de seu cargo ou função. A concessão da credencial de acesso permite ao usuário interno acessar a *internet* e as informações corporativas pelo uso de recursos tecnológicos cedidos pela Semove

que possuam infraestrutura gerida pelas áreas de negócios competentes. Em caso de conselheiros, delegados dos sindicatos, esta solicitação, quando requerida, é realizada pela Diretoria Jurídica/Coordenação Jurídica; em caso de representantes do CIC, esta solicitação, quando requerida, é realizada pela Gerência de Controles Internos e Riscos.

7.2. O usuário (interno ou externo) deverá assinar os Termos de Recebimento e Uso dos recursos tecnológicos que lhe foram disponibilizados pela Semove, além de anuir com o **Termo de Aceite** desta Norma (ANEXO I e ANEXO II) e demais instrumentos normativos, que devem ser guardados em local seguro pelas áreas de negócios competentes.

7.3. O Termo de Aceite - Pessoa Física (ANEXO I) deve ser retido sob guarda física ou eletrônica da Gerência de Segurança da Informação, com o apoio da Gerência de Controles Internos e Riscos, em local seguro, enquanto o colaborador, gestor, diretor ou presidente-executivo permanecer com contrato de trabalho com a Semove ou após 3 (três) anos contados da data de término desse contrato de trabalho, quando será excluído, salvo se esses ex-empregados ajuizarem ação em face da Semove. Neste caso, o documento ficará armazenado até o término da ação. Por outro lado, o Termo de Aceite - Pessoa Jurídica (ANEXO II) deverá ser mantido pelo gestor competente enquanto for mantido o contrato, acordo, convênio ou instrumento correlato com a Semove. Após 5 (cinco) anos contados do término da contratação, esses documentos deverão ser eliminados, de forma segura.

7.4. O usuário interno utilizará recursos tecnológicos corporativos para acessar a *internet,* via rede cabeada ou *wi-fi*, disponível nas dependências da Semove. Caso contrário, deve obrigatoriamente acessar a *internet* via *VPN* provida pela Semove.

7.5. Quando o usuário interno é desligado, ou afasta-se por licença médica por prazo superior a 15 (quinze) dias, a Gerência de Relações do Trabalho deve solicitar a revogação da sua credencial de acesso, via abertura de chamado na Central de Serviços que, automaticamente, direciona o pleito aos responsáveis pela revogação desses acessos. Desse modo, ele não poderá mais acessar a *internet* corporativa.

7.6. O acesso à *internet* pelo usuário externo nas dependências da Semove é permitido, desde que autorizado pelo gestor, diretor ou presidente-executivo contratante. Para esse fim, o usuário externo deve respeitar as boas práticas de segurança e privacidade da informação e assinar os Termos de Aceite desta Norma (ANEXO II) e demais instrumentos normativos publicados na *intranet* e no *website* da Semove.

7.7. Caso o usuário externo necessite acessar a *internet* em função de alguma demanda/projeto, deve fazê-lo via *wi-fi* de visitante, disponível nas dependências da Semove, mediante senha de acesso, que deve ser alterada a cada 3 (três) meses. É vedado ao usuário interno o uso da rede *wi-fi* de visitante, exceto para os agentes de governança.

7.8. Cada acesso concedido, seja ao usuário interno ou externo, deve permitir a sua identificação pessoal, através do uso de credencial e senha única e intransferível, conforme previsto na PSI.

7.9. Cabe à Gerência de Segurança da Informação demandar ao responsável pelos usuários, em bases anuais, a revisão das credenciais de acesso aos recursos tecnológicos corporativos, de modo que os direitos de acesso estejam compatíveis com os cargos, funções e áreas de negócios em que estão alocados, caso contrário, esses acessos deverão ser modificados ou revogados. Consequentemente, esse procedimento previne o mau uso da *internet* provida pela Semove.

8. CONDUTAS PROIBIDAS NO USO DA *INTERNET*

8.1. De forma a tornar responsável o uso da *internet* no trabalho, todos os usuários devem se abster de realizar atividades prejudiciais à Semove (direta ou indiretamente) ou que possam prejudicar os relacionamentos com suas partes interessadas ou relacionadas. Sendo assim, são consideradas práticas proibidas:

a) acessar, divulgar e repassar qualquer material pornográfico, atentatório à moral e aos bons costumes, ofensivo ou discriminatório;

b) acessar, divulgar e repassar qualquer material de incitação à violência, criminoso ou que faça apologia ao crime;

c) acessar, divulgar e repassar qualquer tipo de conteúdo malicioso (i.e., ***malware***) ou programas de controle de outros recursos tecnológicos, sem autorização da Gerência de Infraestrutura/Coordenação de *Service Desk* em conjunto com a Gerência de Segurança da Informação;

d) difamar, caluniar, perturbar, amedrontar, discriminar, praticar *bullying*, ameaçar ou ofender outrem;

e) conteúdo religioso, político-partidário ou eleitoral;

f) anúncios publicitários, mensagens do tipo “corrente”, vírus ou qualquer outro tipo de programa de computador que não seja destinado ao desempenho de suas funções ou que possam ser considerados nocivos ao ambiente de rede da Semove.

g) divulgar “*fake news*”, informação ilícita ou que conflite com os objetivos estratégicos da Semove, prejudicando os relacionamentos com suas partes interessadas e/ou relacionadas;

h) utilizar ***proxy***, *websites* ou qualquer ferramenta correlata que permita anonimizar a identificação do usuário, para acessar conteúdo confidencial não autorizado ou bloqueado pelas soluções de segurança que protegem o acesso à *internet*;

i) instalar arquivos de *softwares*, sistemas e aplicativos não homologados, ainda que seu perfil de usuário seja de administrador de sistemas, em especial arquivos que contenham materiais ilegais, suspeitos ou que não respeitem os direitos autorais;

j) acessar *websites* de jogos de azar ou apostas ou realizar atividades relacionadas a jogos eletrônicos, não compatíveis com o trabalho, cargo ou função que exercem;

k) realizar mineração de criptomoedas;

l) acessar, transferir, compartilhar, importar, armazenar, divulgar informações confidenciais (sigilosas, restritas ou internas) ou públicas sem autorização do Órgão Diretivo;

m) acessar, transferir, compartilhar, importar, armazenar, utilizar, divulgar qualquer informação que contenha dados pessoais (sensíveis ou não), sem autorização;

n) utilizar *e-mail* corporativo para fins pessoais;

o) acessar *internet* provida em locais públicos;

p) compartilhar credenciais e senhas de acesso com terceiros;

q) responder a críticas, esclarecer dúvidas de terceiros ou emitir opinião em nome da Semove nas redes sociais e demais ambientes digitais, sem autorização do Órgão Diretivo;

r) utilizar conteúdo de terceiros sem a devida autorização do proprietário;

s) compartilhar informações confidenciais em recursos tecnológicos de terceiros, especialmente em ambientes digitais não homologados pelas áreas técnicas (ex.: compartilhamento de dados confidenciais em inteligência artificial).

8.2. As situações acima são exemplificativas, portanto, não esgotam o conjunto de infrações previstas na legislação vigente e demais instrumentos normativos ou contratuais da Semove. Cada infração será avaliada individualmente, conforme previsto na Política de Consequências, levando-se em consideração o tipo de infração, impacto, dolo ou culpa do infrator, reincidência etc.

9. SEGURANÇA DA INFORMAÇÃO E AMBIENTE TECNOLÓGICO DA SEMOVE

9.1. Os recursos tecnológicos utilizados para acesso à *internet* devem estar amparados por sistemas de proteção contra *malwares* instalados, ativados e atualizados, de forma a resguardar suas informações.

9.2. O acesso à *internet* deve ser realizado somente por meio de navegadores homologados pela Gerência de Infraestrutura/Coordenação de *Service Desk* em conjunto com a Gerência de Segurança da Informação.

9.3. É responsabilidade da Gerência de Segurança da Informação implementar controles internos que visem prevenir, detectar ou remediar acesso de usuários a *websites* maliciosos ou suspeitos, além de monitorar esses acessos.

9.4. Caso o usuário identifique o bloqueio de segurança em um *website* necessário para o trabalho, ele poderá abrir um chamado via Central de Serviços para que a Gerência de Segurança da Informação avalie a revogação do bloqueio.

9.5. A Gerência de Segurança da Informação, com o suporte da Gerência de Desenvolvimento Organizacional, investe em programas de treinamento contínuo, em bases mensais, visando à capacitação de usuários internos nas boas práticas de segurança da informação.

9.6. É compromisso do Órgão Diretivo, com o apoio da Gerência de Segurança da Informação, expandir esses treinamentos aos usuários externos, que habitualmente, por força de contrato, convênio, acordo, utilizem os recursos tecnológicos corporativos. Embora essas relações possam estar amparadas por acordos de confidencialidade celebrados com a Semove, os usuários externos, quando não instruídos adequadamente em relação às boas práticas de segurança e privacidade da informação, podem sofrer processos de responsabilização legal por mau uso da *internet*, além de submeter a pessoa jurídica que representam a sanções contratuais, quando constatada sua culpabilidade em relação à ocorrência de incidentes de segurança da informação que impactem significativamente a Semove.

10. MONITORAMENTO E AUDITORIA

10.1. A Semove, através das áreas que visam avaliar a conformidade em relação à segurança e à privacidade da informação, reserva-se o direito de monitorar, investigar e auditar, sem necessidade de aviso prévio ou de consentimento do usuário, o uso dos recursos tecnológicos corporativos. Isto inclui todos os acessos à *internet*, bem como as informações armazenadas em computadores, *notebooks*, aparelhos celulares, demais dispositivos móveis, nas redes e nos *drives*.

10.2. Em respeito ao direito à privacidade, é proibido o monitoramento, sem consentimento prévio do usuário, de recursos tecnológicos privados. Em situações de quebra de sigilo, em razão de requerimento judicial pleiteado por autoridades fiscalizadoras, o tratamento será dado conforme a legislação e o ordenamento jurídico próprio.

10.3. A Gerência de Segurança da Informação deve demandar que as áreas de negócios contratantes ou desenvolvedoras de sistemas, *softwares* ou aplicativos assegurem, desde a concepção, condições de rastrear as atividades dos seus usuários (ex.: *logs* ou relatórios de auditoria), proteção das informações contra crimes cibernéticos, procedimentos de autenticação de usuários, criptografia de dados etc. Nesse sentido, a Semove deve investir ou desenvolver ferramentas que contemplem essas funções, rastreando as ações dos usuários na *internet*, bem como criptografando seus dados de navegação na *web*. Os *logs* de acesso à *internet* devem ser mantidos por 1 (um) ano, para servir como evidência em futuras investigações.

10.4. Todo usuário deve ter cautela ao navegar na *internet*, para evitar a divulgação de informações confidenciais ou, até mesmo, informações públicas ainda não autorizadas pelo Órgão Diretivo da Semove.

10.5. Também, em razão de investigações de atos suspeitos, ilícitos ou em desconformidade com instrumentos normativos publicados, a Semove se reserva o direito de monitorar conteúdos privados tornados públicos pelos próprios usuários na *internet* (i.e., redes sociais e demais ambientes digitais) com o intuito de avaliar e remediar possíveis danos à sua imagem, reputação e aos negócios firmados com suas partes interessadas e relacionadas, conforme Norma de Boas Práticas nas Redes Sociais e Demais Ambientes Digitais.

10.6. A Gerência de Segurança da Informação é responsável por definir os critérios e parâmetros de bloqueio automático de conteúdo na *internet*, restringindo acesso a *websites* inseguros, fraudulentos, maliciosos e/ou inúteis para fins de trabalho, bloqueando tentativas reiteradas de instalações de *softwares* suspeitos ou ainda não homologados pelas áreas técnicas da Gerência de Infraestrutura/Coordenação de *Service Desk* e da Gerência de Segurança da Informação.

11. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

11.1. Os incidentes de segurança da informação podem ser causados por: i) ataques externos (ex.: ***phishing***, ***ransomware*** etc.) frente às vulnerabilidades dos sistemas da Semove (ex.: *software* desatualizado); ii) falha nas soluções de segurança da informação (ex.: não bloqueio automático de *websites* inseguros, maliciosos ou fraudulentos); iii) culpa ou dolo do usuário (interno ou externo) quanto ao uso seguro da *internet* (ex.: instalação de *malware*, adoção de senhas inseguras, compartilhamento de credenciais de acesso e senha etc.); ou iv) ausência de controle eficaz de acesso físico às dependências da Semove, dando ao **cibercriminoso** acesso aos recursos tecnológicos corporativos disponíveis nas estações de trabalho (ex.: ***tailgating***).

11.2. Todo incidente de segurança da informação (potencial ou confirmado) precisa ser comunicado imediatamente à Gerência de Segurança da Informação inicialmente por telefone, *chat* do *Google* ou qualquer outro meio mais célere, desde que haja, por parte do relator, a confirmação inequívoca do recebimento deste aviso por parte da Gerência de Segurança da Informação, para que haja tempo hábil de reação e, consequentemente, mitigação tempestiva do seu impacto.

Posteriormente, é necessário formalizar o fato por meio do *e-mail*: gsi@semove.org.br, Central de Serviços e, sempre que envolver a alta administração, registrar também no Canal de Denúncia e Diálogo Voz Ativa.

11.3. A Gerência de Segurança da Informação se compromete a empreender os melhores esforços para conter tempestivamente qualquer suspeita ou ocorrência de incidentes de segurança da informação. No entanto, se o incidente de segurança da informação prejudicar, de modo **significativo**, a Semove, comprometendo as sua marca, reputação, negócio, operação ou a privacidade dos dados pessoais; ou quando for de complexa resolução diante da infraestrutura disponível no momento da crise, ou não for possível determinar a extensão do seu impacto, caberá à Gerência de Segurança da Informação comunicar imediatamente ao Órgão Diretivo e instaurar, em caráter emergencial, o Grupo de Gestão de Incidentes de Segurança da Informação.

11.4. Neste cenário, caberá ao Órgão Diretivo prover infraestrutura necessária, com o suporte da alta administração e definir os integrantes do Grupo de Gestão de Incidentes de Segurança da Informação. Este, em conjunto com a Gerência de Segurança da Informação, iniciará um plano de ação emergencial para remediar a crise ocasionada por um eventual incidente de segurança da informação até restabelecer o estado de normalidade dos negócios/operações da Semove com as suas partes interessadas ou relacionadas, assumindo o compromisso de prestar contas e comunicar à alta administração, na menor periodicidade possível, o *status* deste plano. Sua execução e condução será feita pelos líderes das áreas de negócios atuantes no nível operacional, tático ou estratégico, cujas ações serão monitoradas pelas áreas de auditoria e suporte, dentre as quais se destacam a Gerência de Auditoria Interna, a Gerência de Controles Internos e Riscos e, quando houver

exposição de dados pessoais, a Gerência de Proteção de Dados e Privacidade. Sempre que o incidente de segurança da informação acarretar dano relevante aos dados pessoais, o gerente de Proteção de Dados e Privacidade deverá intermediar o relacionamento com os titulares de dados pessoais, a **ANPD** e/ou demais órgãos fiscalizadores da proteção e privacidade de dados, conforme previsto na LGPD.

11.5. Caberá às áreas de negócios acionadas pelo Grupo de Gestão de Incidentes de Segurança da Informação envidarem os melhores esforços para cumprirem as ações que lhes forem delegadas, respeitando os valores, princípios organizacionais, a legislação e os instrumentos contratuais ou normativos vigentes, assumindo integral responsabilidade pelas ações implementadas ou omissões.

11.6. A presidência-executiva, com o apoio da Diretoria Jurídica/Coordenação Jurídica e das áreas responsáveis pelos canais de comunicação corporativa, deverá avaliar o momento e a forma de divulgar, para as partes interessadas ou relacionadas afetadas, em caráter de confidencialidade, as medidas emergenciais tomadas para mitigar a crise ou, até mesmo, declarar publicamente o seu cenário.

12. CONSEQUÊNCIAS PUNITIVAS

12.1. Todos devem ser diligentes e responsáveis por suas ações no trabalho, portanto, cada indivíduo, independentemente do cargo/função que ocupe, responde integralmente por qualquer conduta que resulte em danos significativos ao negócio, imagem e reputação da Semove e suas partes interessadas ou relacionadas. Toda conduta ou deliberação que conflite com as diretrizes desta Norma é proibida, portanto, a comprovação de uma infração pode acarretar aplicação de medidas disciplinares ou, em última instância, o ajuizamento de ação de responsabilização

administrativa, civil ou penal contra o colaborador, gestor, diretor ou presidente-executivo que infringir ou incentivar sua violação, conforme Política de Consequências. Para esse fim, a Semove disponibiliza o Canal de Denúncia e Diálogo Voz Ativa (Canal), que permite o registro de relatos anônimos ou identificados nos seguintes canais:

- *Website*: https://www.canalconfidencial.com.br/vozativa/;
- Telefone: 0800 741 0003 (atendimento pessoal, de segunda a sábado, das 12h às 22h);
- *E-mail*: vozativa@canalconfidencial.com.br;
- Caixa postal: 521 CEP 06320-971.

12.2. As diretrizes sobre o funcionamento deste Canal estão previstas na Política do Canal de Denúncia e Diálogo, divulgada nos canais de comunicação da Semove.

13. INSTÂNCIAS CORPORATIVAS DE APROVAÇÕES

13.1. Esta Norma foi revisada pela Gerência de Segurança da Informação e submetida à análise dos representantes do CIC em 07/03/2024.

13.2. Foi aprovada pelos membros do Órgão Diretivo em 10/05/2024 que, no conjunto, autorizaram sua publicação.

13.3. Recomenda-se, como boa prática de governança corporativa, submetê-la a todas as instâncias responsáveis por sua aprovação, sempre que houver alterações significativas em seu conteúdo. Caso contrário, poderá ser publicada com o propósito de se realizarem pequenas atualizações.

14. ANEXOS

14.1. A Norma de Utilização da *Internet* possui os seguintes anexos:

- ANEXO I – Termo de Aceite Pessoa Física.
- ANEXO II – Termo de Aceite - Pessoa Jurídica.
- ANEXO III – Glossário da Norma de Utilização da *Internet.*

14.2. Os anexos são partes integrantes desta Norma, embora sejam divulgados separadamente, pois podem sofrer constantes atualizações.

14.3. Os Termos de Aceite (ANEXO I e II) desta Norma serão mantidos em local seguro, de acordo com o prazo previsto nestes instrumentos contratuais.

14.4. Todos os colaboradores, gestores, diretores e presidente e demais pessoas físicas consideradas partes interessadas ou relacionadas à Semove devem conhecer e assinar os Termos de Aceite desta Norma (ANEXO I), que serão geridos pela Gerência de Segurança da Informação.

14.5. Com intuito de apoiar os gestores na gestão dos Termos de Aceite desta Norma (ANEXO I), a Gerência de Segurança da Informação realizará a coleta de assinaturas eletrônicas dos empregados, por meio de sistema de gestão de instrumentos normativo que os armazenará em local seguro, de acordo com o prazo previsto nestes instrumentos contratuais.

14.6. Caberá ao gestor competente ou seu superior imediato, a coleta de assinaturas dos Termos de Aceite desta Norma (ANEXO II) junto aos empregados que representam suas partes interessadas ou relacionadas, desde que utilizem, para a execução do escopo contratado, a internet para tráfego de informações de propriedade ou custodiadas pela Semove, pois devem conhecer e anuir com as diretrizes desta Norma.

ANEXO I – TERMO DE ACEITE - PESSOA FÍSICA

Pelo presente instrumento ("Termo de Aceite"),_____ [Nome completo do empregado(a) (Declarante)], inscrito(a) no CPF/MF sob o nº [_ _ _ _ _ _._ _ -_ _], empregado(a) da [Federação das Empresas de Mobilidade do Estado do Rio de Janeiro (Requerente)]_____, DECLARA que:

i. Tomou conhecimento e compreendeu as disposições previstas na NOG001.SI.SEM - Norma de Utilização da *Internet*, divulgada nos canais de comunicação da Requerente, se comprometendo a respeitar, no desempenho de suas atividades, todos os seus termos, condições e princípios, estando sujeito(a) às medidas disciplinares cabíveis advindas do descumprimento, sem prejuízo de responder por processos de responsabilização legal;

ii. As diretrizes da Norma de Utilização da *Internet* não se sobrepõem à legislação vigente, convenção, contrato social, regimento interno e, se complementam aos demais instrumentos normativos ou contratuais publicados pela Requerente;

iii. O Termo de Aceite tem o propósito de evidenciar a eficácia dos instrumentos normativos como padrão de conduta de uma organização, pilar específico do Programa de Integridade e Conformidade da Requerente, conforme art. 57, inciso II, do Decreto nº 11.129/2022 (novo Decreto Anticorrupção). Por esse motivo, é importante que o(a) Declarante tome conhecimento, concorde e cumpra com as diretrizes aqui estabelecidas e aprovadas pelo Órgão Diretivo da Requerente, bem como por instâncias superiores de governança corporativa.

iv. Os dados pessoais coletados neste Termo de Aceite serão mantidos pela Requerente pelo tempo necessário ao cumprimento de sua finalidade, conforme tabela abaixo:

Dados pessoais coletados	Finalidade de tratamento de dados pessoais
Nome completo, nº do CPF e o aceite digital do(a) Declarante (campo de preenchimento obrigatório)	Identificar o(a) Declarante que anuiu com as diretrizes desta Norma. O nº do CPF é necessário para se evitar homônimos, ou seja, pessoas com nomes iguais.
E-mail do(a) Declarante (campo de preenchimento obrigatório)	Contatar o(a) Declarante, caso seja necessário. Coletar a assinatura eletrônica do Termo de Aceite desta Norma, além de enviar ao(à) Declarante uma comprovação desta assinatura.

v. Este Termo de Aceite não será compartilhado com terceiros, salvo se decorrer de: i) investigações internas, ii) ação ajuizada no âmbito administrativo ou judicial em face da Requerente ou iii) requerimento legal por parte de órgãos fiscalizadores, situação que não requer consentimento do(a) Declarante.

vi. Este Termo de Aceite será armazenado pela Requerente, de forma segura, enquanto o(a) Declarante permanecer com contrato de trabalho estabelecido com a Requerente ou após 3 (três) anos contados da data de término desse contrato de trabalho, quando será excluído, salvo se for ajuizada ação, pelo(a) Declarante, em face da Requerente. Neste caso, este documento ficará armazenado até o término da ação.

Rio de Janeiro, _____ de _____ de 20___.

Aceite digital do(a) empregado(a) (Declarante)

E-mail corporativo do(a) Declarante:

ANEXO II – TERMO DE ACEITE - PESSOA JURÍDICA

Pelo presente instrumento ("Termo de Aceite"),_____ [Nome completo do(a) empregado(a) (Declarante)], inscrito(a) no CPF/MF sob o nº _ _ _ _ _ _._ _ -_ _ , empregado(a) da (nome da Empresa) [1] _____, inscrito(a) no CNPJ sob o nº_____, DECLARA para a [Semove - Federação das Empresas de Mobilidade do Estado do Rio de Janeiro. (Requerente)]_____, que:

i. Tomou conhecimento e compreendeu as disposições previstas na NOG001.SI.SEM - Norma de Utilização da *Internet*, divulgada nos canais de comunicação da Requerente, se comprometendo a respeitar, no desempenho de suas atividades, todos os seus termos, condições e princípios, estando sujeito(a) às sanções cabíveis advindas do descumprimento, sem prejuízo de responder por processos de responsabilização legal;

ii. As diretrizes da Norma de Utilização da *Internet* não se sobrepõem à legislação vigente, convenção, contrato social, regimento interno e, se complementam aos demais instrumentos normativos ou contratuais publicados pela Requerente;

iii. O Termo de Aceite tem o propósito de evidenciar a eficácia dos instrumentos normativos como padrão de conduta de uma organização, pilar específico do Programa de Integridade e Conformidade da Requerente, conforme art. 57, inciso II, do Decreto nº 11.129/2022 (novo Decreto Anticorrupção). Por esse motivo, é importante que o(a) Declarante tome conhecimento, concorde e cumpra com as diretrizes aqui estabelecidas e aprovadas pelo Órgão Diretivo da Requerente, bem como por instâncias superiores de governança corporativa.

[1] Empresa: refere-se a qualquer pessoa jurídica que estabelecer contrato, acordo, convênio ou instrumento correlato com a Semove (ex.: fornecedores, parceiros comerciais e demais partes interessadas ou relacionadas).

iv. Os dados pessoais coletados neste Termo de Aceite serão mantidos pela Requerente pelo tempo necessário ao cumprimento de sua finalidade, conforme tabela abaixo:

Dados pessoais coletados	Finalidade de tratamento de dados pessoais
Nome completo, nº do CPF e o aceite digital do Declarante (campo de preenchimento obrigatório)	Identificar o(a) Declarante que anuiu com as diretrizes desta Norma. O nº do CPF é necessário para se evitar homônimos, ou seja, pessoas com nomes iguais.
E-mail corporativo do(a) Declarante (campo de preenchimento opcional)	Contatar o(a) Declarante, caso seja necessário. Coletar a assinatura eletrônica do Termo de Aceite desta Norma, além de enviar ao (à) Declarante uma comprovação desta assinatura.

v. Este Termo de Aceite não será compartilhado com terceiros, salvo se decorrer de: i) investigações internas, ii) ação ajuizada no âmbito administrativo ou judicial em face da Requerente ou iii) requerimento legal por parte de órgãos fiscalizadores, situação que não requer consentimento do(a) Declarante.

vi. Este Termo de Aceite será armazenado pela Requerente, de forma segura, enquanto a empresa do(a) Declarante mantiver contrato, acordo, convênio ou instrumento correlato com a Requerente ou por 5 (cinco) anos contados da data de término desta contratação, quando será excluído, salvo as situações previstas no item (v) acima. Neste caso, este documento ficará armazenado até o término destas situações previstas no item precedente.

Rio de Janeiro, _____ de _____ de 20___.

Aceite digital do(a) empregado(a) (Declarante)

E-mail corporativo do(a) Declarante:

ANEXO III – GLOSSÁRIO

Agente de governança: indivíduo que ocupa um papel de liderança no Órgão Diretivo (ex.: diretor ou presidente-executivo) e qualquer membro dos órgãos envolvidos no sistema de governança corporativa (ex.: representantes do CIC, conselheiros do CG, delegados da AGRS). Os agentes de governança têm influência significativa sobre as decisões estratégicas da Semove.

Aparentado por afinidade: refere-se aos parentes originados não por vínculo sanguíneo ou adoção, mas por vínculo matrimonial ou relação afetiva (ex.: cônjuge, companheiro(a), enteado(a), sogro(a) e cunhado(a) ou namorado(a)).

Ativo: compreende bem e direito tangível ou intangível que possua valores econômicos agregados para a Semove, tais como: caixa, conta corrente bancária, aplicações financeiras, títulos e valores mobiliários, direitos a receber, participações societárias, móveis, imóveis, recursos tecnológicos, informações, conhecimentos (*know-how*), marcas, patentes e outros tipos de propriedade intelectual.

Cibercriminoso: indivíduo que usa de técnicas de engenharia social para atacar pessoas físicas ou pessoas jurídicas no ambiente digital. É todo aquele que comete crimes eletrônicos, conforme definido na Lei nº 12.737/2012 e no art. 154A do Código Penal Brasileiro, possuindo como objetivo principal, na grande maioria das vezes, a obtenção de lucro ou vantagem indevida.

Colaborador: indivíduo que exerce atividade laboral, regulamentada por lei específica (ex.: estagiários) ou regulamentada pela CLT (ex.: jovem aprendiz, empregado subordinado aos cargos de gestão e direção).

Comitê de Integridade e Conformidade (CIC): órgão colegiado e fiscalizador instituído pelo Conselho de Gestão no sistema de governança da Semove, no intuito de assessorar seus representantes na implantação do Programa de Integridade e Conformidade. Seus poderes, escopo e composição estão definidos em regimento interno.

Conselho de Gestão (CG): órgão colegiado de governança corporativa responsável pelo direcionamento estratégico, por aprovação dos regimentos internos, contratos/estatutos sociais e suas alterações, orçamentos, contratação e destituição de

diretores-executivos, presidente-executivo, auditores internos, bem como, em suas responsabilidades, manifestar opinião sobre propostas direcionadas à AGRS.

Corporativo: significa um ativo (tangível ou intangível) ou material pertencente à Semove ou a terceiros, mas que esteja sob a custódia da Semove.

Crimes cibernéticos (crimes eletrônicos, crimes digitais, crimes da informática): são fraudes eletrônicas ou delitos no meio digital, conforme definido na Lei nº 12.737/2012 e no art. 154A do Código Penal Brasileiro, que consiste em invadir recurso tecnológico alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do recurso tecnológico, ou instalar vulnerabilidades para obter vantagem ilícita (ex.: crimes no ambiente eletrônico, tais como furto qualificado, estelionato, fraude etc.). É um tipo de incidente de segurança da informação que, quando não mitigado em tempo hábil, é passível de acarretar dano, prejuízo ou transtorno à vítima, que pode ser um indivíduo ou uma empresa.

Dado pessoal: é a informação relacionada a uma pessoa natural, identificada ou identificável, ou seja, quando é possível a identificação, direta ou indireta, da pessoa natural por trás do dado, como, por exemplo: nome, sobrenome, data de nascimento, documentos pessoais (como CPF, RG, CNH, Carteira de Trabalho, passaporte, número do título de eleitor e crachá de acesso corporativo), endereço residencial ou comercial, número de telefone, *e-mail*, número de cartão de crédito, código de matrícula, número do cartão de vale-transporte, *cookies*, credencial de acesso, protocolo de rede (*Internet Protocol* ou *IP*).

Dado pessoal sensível: dado pessoal que possui maior proteção da lei e requer maior cuidado no tratamento, pelo fato de poder gerar alguma discriminação ao titular. São considerados dados pessoais sensíveis aqueles que possam, de alguma forma, vir a ter um caráter discriminatório, quando vinculados a uma pessoa natural, tais como: origem racial ou étnica, convicção religiosa, opinião política, filiação a entidades representativas de caráter religioso, filosófico ou político, dados referentes à saúde ou orientação

sexual, dados genéticos ou biométricos, dados de apoio a entidades de práticas desportivas.

Diretor: indivíduo que ocupa cargo de direção na Semove com o objetivo de executar e cumprir o planejamento estratégico. Quando houver referência ao diretor-executivo, significa o diretor estatutário; caso contrário, significa o diretor celetista.

Dispositivo móvel: equipamento portátil dotado de capacidade computacional ou dispositivo removível de memória para armazenamento, entre os quais se incluem, não se limitando a estes: *notebooks*, celulares, *tablets*, *pendrives*, disco rígido (*Hard Disk* ou *HD* externo) e cartões de memória.

Gestor: indivíduo que ocupa cargo de confiança para gerir uma ou mais áreas de negócios (ex.: coordenadores, supervisores, líderes de loja e gerentes), alocado (direta ou indiretamente) sob a estrutura organizacional de uma Gerência, Diretoria ou da Presidência-Executiva.

Grupo de Gestão de Incidentes de Segurança da Informação: grupo multidisciplinar, liderado pela Gerência de Segurança da Informação**,** responsável por definir e submeter à alta administração um plano de ação estratégico que visa remediar a crise gerada por eventual incidente de segurança da informação, de impacto significativo, até que haja o restabelecimento do estado de normalidade dos negócios da Semove, principalmente preservando e restabelecendo seus relacionamentos com suas partes interessadas ou relacionadas. Esse plano de ação deve ser comunicado pelas equipes estratégicas às equipes atuantes na operação ou negócio-chave, além de ter seu cumprimento monitorado pelas equipes alocadas nas áreas de auditoria e fiscalização.

Incidente de segurança da informação: ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema. Poderá também ser caracterizado pela tentativa de exploração de vulnerabilidade de sistema de informação que caracterize violação de instrumentos normativos e procedimentos de segurança ou de uso. De maneira geral, os tipos de atividade comumente reconhecidas como incidentes cibernéticos são: a) tentativas de obter acesso não autorizado a um sistema ou a dados armazenados; b)

tentativa de utilização não autorizada de sistemas para a realização de atividades de processamento ou armazenamento de dados; c) mudanças não autorizadas de *firmware*, *hardware* ou *software* em um ambiente computacional; d) ataques de negação de serviço (*Denial-of-service attack* ou *DoS*); e e) demais ações que visem afetar a disponibilidade ou integridade dos dados. Um incidente de segurança da informação não significa necessariamente que a informação já esteja comprometida; significa apenas que a informação está ameaçada.

Informação: é o conjunto de dados e conhecimentos organizados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato, incluindo-se os dados que possam constituir referências sobre um determinado indivíduo (i.e., dados pessoais) ou sobre determinado acontecimento, ocorrência ou fenômeno dentro da Semove. A informação é um ativo intangível de propriedade ou custodiado pela Semove, que gera valor para o negócio. Deve estar sempre classificada como pública ou segundo os níveis de confidencialidade: interno, restrito ou sigiloso.

Internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes.

***Malware*:** abreviação de "*software* malicioso" (em inglês, *malicious software*) que se refere a um tipo de programa de computador desenvolvido para infectar os recursos tecnológicos, com o intuito de prejudicar seus usuários, por meio de furto, deleção, modificação, bloqueio de acesso, falsificação de dados e/ou comprometimento do desempenho ou funcionamento do ativo e da rede. Possui diversas formas, entre elas vírus, *worms*, cavalos de Troia, *spam*, *spywares*, dentre outros.

Navegador: é um aplicativo de *software* que permite ao usuário navegar na *internet* (ex.: Google Chrome, Mozilla Firefox, Microsoft Edge, dentre outros).

Órgão Diretivo: é o conjunto formado pelos diretores e presidente-executivo da Semove, responsáveis por liderar e conduzir seus negócios/operações alinhados aos interesses legítimos, íntegros e lícitos da alta administração, respeitando seus valores

organizacionais. Para esse fim, podem atuar em uma ou mais áreas de negócios no nível estratégico, tático ou operacional.

Parente: refere-se aos parentes originários por vínculo sanguíneo ou adoção, tais como pai, mãe, filhos biológicos ou adotivos, irmãos e irmãs. Para mais detalhes, consulte a definição dos artigos 1.591 a 1.595 do Código Civil.

Parte interessada: é toda pessoa física ou pessoa jurídica envolvida, direta ou indiretamente, nos projetos, atividades, negócios e operações da Semove, tais como: colaboradores, gestores, agentes de governança, financiadores, clientes, fornecedores, conveniados, acionistas/cotistas, sindicatos de ônibus, permissionários e concessionários do transporte público do estado do Rio de Janeiro, controladas, coligadas, agentes intermediários, agentes públicos, comunidades, governo, entidades de classe, organizações não governamentais, dentre outros.

Parte relacionada: é toda pessoa física ou pessoa jurídica que, direta ou indiretamente, por meio de um ou mais intermediários:

a) represente ou controle a Semove, direta ou indiretamente, por meio de participações societárias/acionárias majoritárias;
b) seja representada ou controlada pela Semove, direta ou indiretamente, por meio de participações societárias/acionárias;
c) seja empreendimento sob o controle comum da Semove ou de sua controladora, diretamente com outros sócios/acionistas, ou indiretamente, por meio de participações societárias/acionárias;
d) seja coligada direta da Semove, ou indiretamente, por meio de participações societárias/acionárias minoritárias;
e) for um agente de governança, ou parente, ou aparentado por afinidade de agente de governança das empresas enquadradas nos itens (a), (b) e (c) acima, por ter condições de exercer influência significativa nas diretrizes de governança destas empresas, considerando seus respectivos mercados de atuação;
f) for uma empresa de transporte público coletivo de passageiros, no modal ônibus, que firme contrato ou acordo com a Semove, na qualidade de fornecedora, cliente, parceira comercial ou conveniada (excetuadas as

operações de ressarcimento das transações de mobilidade urbana às operadoras de transporte processadas no sistema de bilhetagem eletrônica);

g) toda parte relacionada à Semove é considerada parte interessada, mas nem toda parte interessada é relacionada. Para mais detalhes, consultar o pronunciamento do CPC, nº 05 (R1)/2008 - Divulgação sobre Partes Relacionadas.

***Phishing*:** é uma técnica de crime cibernético que usa a engenharia social para enganar vítimas, manipulando-as para que cliquem em *links*/arquivos maliciosos ou divulguem informações pessoais confidenciais, por meio de mensagens de *e-mail*. Se o *phishing* ocorrer por meio de mensagens de *SMS*, fica categorizado como "*smishing*". Se o *phishi*ng for direcionado a um indivíduo específico, fica categorizado como "*spear phishing*".

Presidente-executivo: é o líder máximo do Órgão Diretivo e contratado sob regime do Contrato Individual de Trabalho. Quando denominado "presidente-executivo", significa que também possui atribuições previstas nos estatutos da Semove, que se reporta diretamente ao CG e indiretamente à AGRS.

Proxy: é uma solução de tecnologia que funciona como um intermediário entre o dispositivo do usuário e os serviços de *internet* que ele acessa. Ele direciona o tráfego de cada aparelho por uma rota específica, a partir das configurações do usuário. Desse modo, é possível bloquear *websites*, gerar mais privacidade para a navegação e evitar situações de risco.

Ransomware: é um tipo de código malicioso que torna inacessíveis os dados armazenados em um recurso tecnológico, geralmente usando criptografia, e que exige pagamento de resgate para restabelecer o acesso ao usuário. O pagamento do resgate geralmente é cobrado em criptomoedas.

Recursos tecnológicos: são ativos e direitos tangíveis ou intangíveis, de natureza tecnológica, utilizados como meios de armazenamento, processamento, comunicação, transmissão de dados e/ou voz. Podem ser privados, corporativos ou de terceiros. Os recursos tecnológicos tangíveis possuem uma forma física, tais como: equipamentos, máquinas, *hardwares*, *notebooks*, computadores, *tablets*, aparelhos celulares, placas de

rede, servidores ativos de conectividade etc. Os recursos tecnológicos intangíveis carecem de forma física, pois são ativos digitais, tais como: licenças de *softwares*, patentes, conhecimentos (*know-how*), direitos autorais de sistemas, rede ou outros tipos de propriedade intelectual.

Significativo(a): o termo refere-se, quando mensurável, a algo que tenha valor material em termos monetários ou a algum fato ou acontecimento relevante, capaz de influenciar a tomada de decisão pelo Órgão Diretivo ou instâncias superiores de governança da Semove com o propósito de proteger seus interesses legítimos e lícitos, preservando sua imagem, reputação e as diretrizes operacionais, táticas ou estratégicas dos seus negócios.

***Software*:** é um programa, sistema ou aplicativo instalado nos computadores ou dispositivos móveis.

***Tailgating*:** é uma técnica física de engenharia social, que ocorre quando um cibercriminoso segue algum indivíduo autorizado até as dependências da Semove, de acesso restrito aos empregados e convidados autorizados, explorando a boa vontade ou distração dos empregados, com o objetivo de obter acesso a ativos valiosos e/ou informações confidenciais.

Termo de Aceite: acordo assinado pelos colaboradores, gestores, diretores, presidente-executivo e demais partes interessadas ou relacionadas à Semove, pelo qual assumem, de forma livre, informada e inequívoca, o compromisso de conhecer e cumprir as diretrizes desta Norma.

Termo de Devolução: acordo assinado pelos usuários/custodiantes dos recursos tecnológicos com a lista dos ativos e acessórios devolvidos, que estavam sob sua guarda para uso em suas atividades profissionais, no qual fica registrado seu compromisso de ressarcimento à proprietária, em caso de danos causados pelo mau uso, não devolução, furto/roubo sem boletim de ocorrência.

Termo de Recebimento e Uso: acordo assinado pelos usuários/custodiantes dos recursos tecnológicos ou mobiliários ergonômicos cedidos pela Semove para o exercício de suas atividades profissionais, em que constam a lista dos ativos e acessórios e o compromisso de protegê-los, mantê-los e conservá-los.

Usuário: é o indivíduo que possui autorização de acesso aos recursos tecnológicos para execução de suas atividades profissionais. O usuário pode ser categorizado como usuário interno, quando a credencial de acesso aos recursos tecnológicos tem domínio corporativo "@semove.org.br", caso contrário, será categorizado como usuário externo.

Virtual private network **(*VPN*)**: ferramenta que estabelece uma conexão de rede protegida ao usar redes públicas. As *VPNs* criptografam seu tráfego de *internet* e disfarçam sua identidade *on-line*.