TRENSURB

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA TRENSURB

Identificação Geral

Empresa de Trens Urbanos de Porto Alegre S.A.
CNPJ: 90.976.853/0001-56, NIRE: 43500317874
Sede: Porto Alegre/RS
Natureza Jurídica: Empresa Pública
Acionista controlador: União
Abrangência de atuação: Região Metropolitana de Porto Alegre
Setor de atuação: Transporte Público Coletivo Ferroviário

Conselheiros de Administração:
Ricardo Hingel - Presidente
Roberta Zanenga de Godoy Marchesi
Clóvis Felix Curado Junior
Fabiana Magalhães Almeida Rodopoulos
Ronald Krummenauer
Leonardo Miranda Freitas (representante dos empregados)

Administradores:
Pedro Bisch Neto - Diretor-Presidente
Geraldo Luís Felippe - Diretor de Administração e Finanças
Nélson Lídio Nunes – Diretor de Operações

Elaboração:
Gerência de Informática - GEINF

Aprovação:
CONSAD, Ata n°. 522, de 27 de janeiro de 2023.
Resolução do Conselho de Administração nº 0001/2023.
Data da divulgação: 14/02/2023.

Política de Gestão Integrada de Riscos Corporativos TRENSURB

Capítulo I - Finalidade e abrangência

Art 1. A Política de Segurança da Informação - PSI - tem por finalidade assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação a nível organizacional, no âmbito da TRENSURB.

Art. 2. Definir e regulamentar medidas aos ativos de informação da TRENSURB, com vistas ao resguardo da imagem e dos objetivos institucionais da Empresa.

Art. 3. Esta Política de Segurança da Informação, assim como os documentos que a compõem, se aplica aos empregados, estagiários, prestadores de serviço, consultores externos e a toda e qualquer pessoa que tenha acesso aos ativos de informação da TRENSURB de forma direta ou indireta.

Capítulo II - Fundamentação legal

Art. 4. Para fins desta Política, considera-se:

I. Decreto Nº 9.637, de 26 de Dezembro de 2018 - Política Nacional de Segurança da Informação - PNSI

II. Decreto nº 10.641, de 2 de março de 2021, altera Decreto nº 9.637/2018.

III. Decreto nº 10.222, de 5 de fevereiro de 2020 - Estratégia Nacional de Segurança Cibernética

IV. Instrução Normativa nº 1, de 27 de maio de 2020 - Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal

V. ABNT ISO/IEC 27001:2013

VI. ABNT ISO/IEC 27002:2013

VII. NPG-PES-702 – Regulamento de Pessoal da TRENSURB

VIII. Código de conduta.

Capítulo III - Conceitos e Definições

Art. 5. Rede Corporativa: é um sistema de transmissão de dados que transfere informações entre diversos equipamentos, com a finalidade de estabelecer comunicação entre pessoas e máquinas, propagando informações diversas, necessárias à operação da TRENSURB. Dentro da empresa a rede transfere informações entre as diversas estações de trabalho, tais como computadores, servidores, impressoras, câmeras de vídeo, e entre alguns desses equipamentos e o ambiente externo.

Art. 6. Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

Art. 7. Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

Art. 8. Ativo: tudo aquilo que possui valor para o órgão ou entidade;
Art. 9. Ativos de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
Art. 10. Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
Art. 11. Capacitação em Segurança da Informação: saber o que é segurança da informação aplicando em sua rotina pessoal e profissional, servindo como multiplicador sobre o tema, aplicando os conceitos e procedimentos na organização;
Art. 12. Confidencialidade: propriedade de que a informação não esteja disponível ou revelada à pessoa física, à sistema, à órgão ou entidade não autorizado e credenciado;
Art. 13. Continuidade de Negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;
Art. 14. Controle de Acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;
Art. 15. Custodiante: responsável por armazenar e preservar as informações que não lhe pertencem, mas que estão sob sua custódia;
Art. 16. Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
Art. 17. Evento: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação; 3.1.14. Gestão de Riscos de Segurança da Informação: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;
Art. 18. Gestão de Segurança da Informação: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação;
Art. 19. Incidente de segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;
Art. 20. Informação Estratégica: toda a informação corporativa relativa à administração, planejamento, estrutura, gestão, relações internas e externas, novos produtos e tecnologias, serviços e contratos; (verificar PNSI)
Art. 21. Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
Art. 22. Política de Segurança da Informação: documento aprovado pela autoridade responsável do órgão ou entidade, com o objetivo de fornecer diretrizes, critérios e suporte administrativos suficientes à implementação da segurança da informação;
Art. 23. Terceiro: pessoa, não integrante do órgão ou entidade, envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso;

Art. 24. Quebra de Segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;
Art. 25. Riscos de Segurança da Informação: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;
Art. 26. Segurança da Informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
Art. 27. Usuário de recursos de Tecnologia da Informação (TI): empregados, prestadores de serviço, estagiários, terceiros e consultores externos que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade, formalizada por meio da assinatura do Termo de Responsabilidade;
Art. 28. Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação;

Capítulo IV - Princípios e Objetivos

Art. 29. Esta política e as subsequentes normas estão adequadas às necessidades e riscos específicos da operação da TRENSURB. O conjunto de documentos que compõe esta política deverá se guiar pelos seguintes princípios:

I. Menor privilégio: Usuários e sistemas devem ter a menor autoridade e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

II. Segregação de função: Funções de planejamento, execução e controle devem ser segregadas de forma a reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos.

III. Auditabilidade: Todos os eventos significantes de sistemas e processos devem ser rastreáveis até o evento inicial.

IV. Mínima dependência de Informação Sigilosa: Os controles deverão ser efetivos ainda que a ameaça saiba de sua existência e como eles funcionam.

V. Controles automáticos: Sempre que possível, os controles de segurança automáticos deverão ser utilizados, especialmente os controles que dependem da vigilância humana e do comportamento humano.

VI. Resiliência: Os sistemas e processos devem ser projetados para que possam resistir ou se recuperarem dos efeitos de um desastre.

VII. Defesa em profundidade: Controles devem ser desenhados em camadas de tal forma que quando uma camada de controle falhar haja um tipo diferente de controle em outra camada para prevenir a brecha de segurança.

VIII. Exceção aprovada: Exceções à política deverão sempre ter aprovação superior.

IX. Substituição da segurança em situações de emergência: Controles somente devem ser desconsiderados de formas predeterminadas e seguras. Devem sempre existir procedimentos e controles alternativos para minimizar o nível de risco em situações de emergência.

X. Educação como alicerce fundamental para o fomento da cultura em segurança da informação.

XI. Orientação à gestão de riscos e à gestão da segurança da informação.

XII. Prevenção e tratamento de incidentes de segurança da informação.

XIII. Articulação entre as ações de segurança cibernética, de proteção de dados e ativos da informação.

XIV. Dever dos órgãos, das entidades e dos agentes públicos de garantir o sigilo das informações imprescindíveis à segurança da sociedade e do Estado e a inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas.

XV. Necessário conhecimento (*need to know*) para o acesso à informação sigilosa, nos termos da legislação.

Art. 30. Esta política tem como objetivo:

I. Aprimorar continuamente o arcabouço normativo relacionado à segurança da informação na empresa;

II. Fomentar a formação e a qualificação dos recursos humanos necessários à área de segurança da informação;

III. Fortalecer a cultura da segurança da informação na empresa;

IV. Orientar ações relacionadas a:

a) Garantir o grau de confidencialidade, integridade e disponibilidade adequado para cada informação produzida, custodiada e/ou sob responsabilidade da TRENSURB;

b) Segurança da informação das infraestruturas críticas;

c) Reduzir os riscos decorrentes da utilização incorreta ou descuidada dos Ativos de Informação;

d) Proteger as informações da TRENSURB, bem como seus ativos computacionais;

e) Proteção das informações das pessoas físicas que possam ter sua segurança ou a segurança das suas atividades afetada, observada a legislação específica;

f) Permitir a integração da TRENSURB, por meio da adoção de critérios conhecidos e previamente acordados de medição dos riscos e ameaças envolvidos no processo.

g) Permitir a integração com parceiros externos, garantindo a integridade das informações e sistemas computacionais dos participantes.

Capítulo V - Competências

Art. 31. Cabe **a todos os empregados**, estagiários, prestadores de serviços, consultores externos e terceiros da TRENSURB:

I. Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação da TRENSURB;

II. Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;

III. Assinar Termo de Responsabilidade, formalizando a ciência e o aceite da Política e das Normas de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento;

IV. Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela TRENSURB;

V. Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela TRENSURB;

VI. Adicionalmente, são definidas as seguintes responsabilidades e atribuições específicas relacionadas à segurança da informação:

Art. 32. Cabe à **Alta Administração** a responsabilidade:

I. Designar gestor de segurança da informação interno, subordinado ao Titular da unidade de Tecnologia da Informação;

II. Instituir comitê de segurança da informação ou estrutura equivalente, para deliberar sobre os assuntos relativos à Política Nacional de Segurança da Informação - PNSI;

III. Destinar recursos orçamentários e humanos para ações de segurança da informação;

IV. Promover a simplificação administrativa, a modernização da gestão pública e a integração dos serviços públicos, especialmente aqueles prestados por meio eletrônico, com vistas à segurança da informação;

V. Monitorar o desempenho e avaliar a concepção, a implementação e os resultados da sua política de segurança da informação e das normas internas de segurança da informação;

VI. Incorporar padrões elevados de conduta para a garantia da segurança da informação e orientar o comportamento dos empregados, em consonância com as funções e as atribuições de seus órgãos e de suas entidades;

VII. Aprovar o planejamento da execução de programas, de projetos e de processos relativos à segurança da informação;

VIII. Estabelecer diretrizes para o processo de gestão de riscos de segurança da informação;

IX. Observar as normas que estabelecem requisitos e procedimentos para a segurança da informação publicadas pelo Gabinete de Segurança Institucional da Presidência da República;

X. Implementar controles internos fundamentados na gestão de riscos da segurança da informação;

XI. Instituir um sistema de gestão de segurança da informação;

XII. Implantar mecanismo de comunicação imediata sobre a existência de vulnerabilidades ou incidentes de segurança que impactem ou possam impactar os serviços prestados ou contratados pelos órgãos da administração pública federal; e

XIII. Observar as normas e os procedimentos específicos aplicáveis, implementar e manter mecanismos, instâncias e práticas de governança da segurança da informação em consonância com os princípios e as diretrizes estabelecidas neste Decreto e na legislação.

Art. 33. Cabe à **GEINF** a responsabilidade:

I. Encaminhar providências necessárias para a implementação das práticas de segurança da informação;

II. Elaborar e propor planejamento da execução de programas, de projetos e de processos relativos à segurança da informação;

III. Elaborar e propor Normas e Procedimentos de Segurança da informação;

IV. Fazer cumprir todas as normas, diretrizes e procedimentos contidos nesta política ou em seus anexos;

V. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

VI. Promover a cultura de segurança da informação através dos seguintes procedimentos:

VII. Propor recursos necessários às ações de segurança da informação;

VIII. Realizar e acompanhar estudos e novas tecnologias, quanto a possíveis impactos na segurança da informação;

IX. Coordenar a Gestão de Riscos de Segurança da Informação;

X. Coordenar a instituição, implementação e manutenção da infraestrutura necessária às equipes que cuidarão dos incidentes relacionados à Segurança da Informação;

XI. Implementação dos Termos de Responsabilidade e procedimentos relativos ao uso dos recursos, em conformidade com as orientações contidas nas Normas Complementares.

XII. Propor ações de treinamento e atualização necessárias;

XIII. Avaliar periodicamente o cumprimento da política de segurança da informação, conforme os critérios sugeridos e homologados pela GEINF.

Art. 34. Cabe ao **GEREH** a responsabilidade:

I. Exigir para todos os empregados e estagiários a assinatura do Termo de Responsabilidade respectivo à função exercida, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da TRENSURB.

II. Garantir ações de capacitação e profissionalização dos recursos humanos em temas relacionados à segurança da informação.

Art. 35. Compete ao **Comitê de Segurança da Informação**

I. Fica instituído o Comitê de Segurança da Informação com atribuições contidas no Comitê Gestor de Tecnologia da Informação de nível Tático.

II. O Gestor da Segurança da Informação será membro efetivo do Comitê de Segurança da Informação.

III. O Comitê de Segurança da Informação terá as seguintes atribuições:

a) Assessorar na implementação das ações de segurança da informação;

b) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

c) Propor alterações na política de segurança da informação interna;

Capítulo VI - Disposições complementares

Art. 36. Esta Política de Segurança da Informação, assim como os demais documentos acessórios que a compõe e leis que regulamentam as suas atividades, são aplicáveis e devem ser obedecidas por todos os empregados, estagiários, prestadores de serviço, consultores externos e toda e qualquer pessoa que tenha acesso aos ativos de informação da TRENSURB de forma direta ou indireta, sendo responsabilidade de cada um o seu cumprimento.

Art. 37. Comissões de Segurança da Informação podem ser implementadas, fornecendo o suporte às ações institucionais estratégicas, priorizando e conduzindo a elaboração e manutenção de uma política de segurança da informação coesa, que possa ser gradualmente efetivada e sirva como referência a questões de segurança da informação.

Art. 38. Incidentes que afetam a segurança das informações, assim como o descumprimento desta política de segurança da informação, devem ser reportados à GEINF para as devidas providências legais e administrativas.

Art. 39. O cumprimento da política de segurança da informação será avaliado periodicamente, de acordo com os critérios sugeridos e homologados pela GEINF.

Art.40. Toda e qualquer informação criada, armazenada ou descartada pelos abrangidos é considerada seu patrimônio e deve ser protegida conforme estabelecido na política de segurança da informação.


TRENSURB