PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

2025

Companhia de Desenvolvimento, Turismo e Inovação de Vitória

PREFEITURA DE VITÓRIA

Aprovada em 22/09/2025

Prefeito Municipal

Lorenzo Silva de Pazolini

Vice Prefeita Municipal

Cris Samorini

Diretor Presidente

Marcus Gregório Serrano

Diretora Administrativo-Financeiro

Donatila Lima Nava Martins

Equipe Técnica de Elaboração

Klaus Kly Cozzuolo Wolff Mischiatti

João Pereira Gomes Netto

João Pedro Barroso Ernesto

SUMÁRIO

CAPÍTULO I – PROPÓSITO 5
CAPÍTULO II – ESCOPO 5
CAPÍTULO III – CONCEITOS E DEFINIÇÕES 5
CAPÍTULO IV – OBJETIVOS 6
CAPÍTULO V – REFERÊNCIAS LEGAIS E NORMATIVAS 7
CAPÍTULO VI – PRINCÍPIOS 7
CAPÍTULO VII – DIRETRIZES GERAIS 8
Seção I. Tratamento da Informação 8
Seção II. Gestão de Incidentes 9
Seção III. Gestão de Ativos 11
Seção IV. Controles de Acesso 13
Seção V. Acesso à Internet 16
Seção VI. E-mail Corporativo 17
Seção VII. Dispositivos Móveis 18
CAPÍTULO VIII – GESTÃO DE SEGURANÇA DA INFORMAÇÃO 20
CAPÍTULO IX – DAS VEDAÇÕES 21
CAPÍTULO X – PENALIDADE 22
CAPÍTULO XI – DISPOSIÇÕES FINAIS 22

Histórico de Versão

Data	Versão	Descrição	Autor
22/09/2025	1.0	Elaboração e publicação da primeira versão da Política de Segurança da Informação institucional, estabelecendo diretrizes, responsabilidades e controles para proteção dos ativos de informação.	Equipe Técnica de Elaboração

CAPÍTULO I – PROPÓSITO

Art. 1º. Esta Política de Segurança da Informação (PSI) tem como objetivo estabelecer os princípios, diretrizes, responsabilidades e práticas para a proteção das informações da Companhia de Desenvolvimento, Turismo e Inovação de Vitória (CDTIV).

Parágrafo único. A PSI visa garantir a confidencialidade, integridade e disponibilidade das informações, assegurando o seu uso adequado e a mitigação de riscos à segurança da informação, bem como o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) e de outras normas vigentes.

CAPÍTULO II – ESCOPO

Art. 2º. Este documento institui no âmbito da CDTIV, com a finalidade de estabelecer princípios e diretrizes para a implementação de ações e controles que garantam a segurança das informações e de dados pessoais, e no que couber, no relacionamento com outras entidades públicas ou privadas.

Art. 3º. Esta PSI se aplica a todos os ativos de informação da CDTIV, incluindo dados, sistemas, aplicativos, dispositivos e redes. A PSI se aplica a todos os servidores, funcionários, contratados, parceiros e terceiros que acessam ou processam as informações da CDTIV. Esta PSI se aplica em todas as instalações físicas administradas ou utilizadas pela CDTIV.

CAPÍTULO III – CONCEITOS E DEFINIÇÕES

Art. 4º. Para efeito desta PSI, considera-se:

I. ATIVO DE INFORMAÇÃO: equipamentos (hardware), programas (softwares) e as informações por eles geradas;
II. CONFIDENCIALIDADE: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;
III. DADO PESSOAL: informação relacionada a pessoa natural identificada ou identificável;
IV. DADO PESSOAL SENSÍVEL: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
V. DISPONIBILIDADE: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

VI. DISPOSITIVO MÓVEL: qualquer equipamento eletrônico com atribuições de mobilidade, de propriedade da CDTIV ou de propriedade particular, a exemplo de notebooks smartphones, tablets, televisores e sistemas de assistentes virtuais inteligentes;

VII. ENCARREGADO: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

VIII. INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

IX. INCIDENTE DE SEGURANÇA: qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, como acesso não autorizado, acidental ou ilícito, que resulte na destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita, a qual possa ocasionar risco para os direitos e liberdades do titular dos dados pessoais, observados os princípios da proporcionalidade e razoabilidade;

X. INTEGRIDADE: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XI. SEGURANÇA DA INFORMAÇÃO: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XII. TITULAR DO DADO: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

XIII. USUÁRIO: pessoa física ou jurídica que se utiliza de qualquer ativo de informação da CDTIV, de forma autorizada, podendo ser um servidor ou prestador de serviços.

CAPÍTULO IV – OBJETIVOS

Art. 5º. São objetivos desta PSI de Segurança da Informação:

I. estabelecer princípios e diretrizes a fim de proteger ativos de informação e conhecimentos gerados ou recebidos;

II. estabelecer orientações gerais de segurança da informação e, desta forma, contribuir para a gestão eficiente dos riscos, limitando-os a níveis aceitáveis, bem como preservar os princípios da disponibilidade, integridade, confiabilidade e autenticidade das informações;

III. estabelecer competências e responsabilidades quanto à segurança da informação;

IV. nortear a elaboração das normas necessárias à efetiva implementação da segurança da informação;

V. promover o alinhamento das ações de segurança da informação com as estratégias de planejamento organizacional da CDTIV.

Parágrafo único. Para os efeitos desta PSI e de suas regulamentações, aplicam-se os termos do Glossário de Segurança da Informação, aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021.

CAPÍTULO V – REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 6º. Esta Política de Segurança da Informação está fundamentada, sem prejuízo de outras legislações aplicáveis, nos seguintes normativos:

I. Lei n.º 12.527, de 18 de novembro de 2011 – Lei de acesso à informação (LAI);
II. Lei n.º 12.965, de 23 de abril de 2014 – Lei do Marco Civil da Internet;
III. Lei n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), e altera a Lei n.º 12.965, de 23 de abril de 2014 que dispõe sobre o Marco Civil da Internet;
IV. Decreto n.º 9.637 de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;
V. Instrução Normativa n.º 1, de 27 de maio e 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal (GSI);
VI. Decreto n.º 23.636 de 23 de maio de 2024, que regulamenta a aplicação e implementação da Lei Geral de Proteção de Dados Pessoais, no âmbito da administração direta e indireta do Poder Executivo Municipal;
VII. Resolução n.º 01/2025 de 02 de maio de 2025, que o Comitê de Proteção de Dados Pessoais (CPDP) estabelece diretrizes para a proteção de dados pessoais no âmbito da administração direta e indireta do Poder Executivo Municipal, conforme a LGPD.

CAPÍTULO VI – PRINCÍPIOS

Art. 7º. As ações de segurança da informação da CDTIV são norteadas pelos princípios constitucionais e administrativos que norteiam a Administração Pública Municipal, bem como pelos seguintes princípios:

I. disponibilidade, integridade, confidencialidade e autenticidade das informações;
II. continuidade dos processos e serviços essenciais para o funcionamento da CDTIV;
III. economicidade da proteção dos ativos de informação;
IV. respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade;
V. observância da publicidade como preceito geral e do sigilo como exceção;

VI. responsabilidade do Usuário de informação pelos atos que comprometam a segurança dos ativos de informação;
VII. alinhamento estratégico da PSI com o planejamento estratégico da CDTIV, assim como demais normas específicas de segurança da informação da Administração Pública Municipal;
VIII. conformidade das normas e das ações de segurança da informação com a legislação regulamentos aplicáveis; e
IX. educação e comunicação como alicerces fundamentais para o fomento da cultura e segurança da informação.

Art. 8. Estas diretrizes constituem os principais pilares da gestão de segurança da informação norteando a elaboração de políticas, planos e normas complementares no âmbito da CDTIV e objetivam a garantia dos princípios básicos de segurança da informação estabelecidos nesta PSI.

Art. 9. As normas, procedimentos, manuais e metodologias de segurança da informação da CDTIV devem considerar, como referência, além dos normativos vigentes, as melhores práticas de segurança da informação.

Art. 10. As ações de segurança da informação devem:

I. considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade da CDTIV;
II. ser tratadas de forma integrada, respeitando as especificidades e a autonomia das unidades da CDTIV;
III. ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação;
IV. visar à prevenção da ocorrência de incidentes.

CAPÍTULO VII – DIRETRIZES GERAIS

Art. 11. A Gestão da Segurança da Informação é constituída, no mínimo, pelos seguintes processos:

Seção I. Tratamento da Informação

Art. 12. Toda informação criada, recebida ou sob a guarda do agente público no exercício de suas funções na CDTIV será considerada um ativo de informação. Esses ativos deverão ser protegidos conforme as legislações e regulamentações de segurança da informação aplicáveis, observando os princípios de confidencialidade, integridade, disponibilidade e autenticidade. O objetivo é mitigar riscos associados às atividades e serviços realizados pela CDTIV ou por terceiros em seu nome.

Art. 13. O tratamento da informação para com as questões decorrentes da LGPD, deverá ser objeto de normativa própria e segundo a legislação aplicável e competente para tal.

Art. 14. Todos os formulários devem ser revisados, digitais ou físicos, visando coletar apenas os dados pessoais estritamente necessários para o cumprimento da finalidade do serviço público, facilitando a ação de inventário e mapeamento de dados da CDTIV.

Art. 15. Tratar dados pessoais ou sensíveis de servidores ou cidadãos somente quando amparado por base legal ou necessidade comprovada.

Art. 16. Garantir o descarte seguro de documentos físicos e digitais contendo dados pessoais.

Art. 17. Assegurar que documentos legais ao exemplo de editais e contratos, bem como ao preencher formulários de sistemas que são publicados para acesso público (Sítio Oficial do Município, Diário Oficial, Portal Transparência, sítio eletrônico da CDTIV, entre outros), tenham os CPF's parcialmente mascarados.

Parágrafo único. Deve ser substituído os cinco primeiros e dois últimos dígitos por asteriscos (Exemplo: ***. **6. 784-**') ou ocultados via tarjamento, inclusive na assinatura digital.

Art. 18. Em caso de dúvidas sobre o tratamento de dados pessoais:

I. o Usuário deverá comunicar o Encarregado pelo Tratamento dos Dados Pessoais via encarregado.lgpd@cdtiv.com.br;
II. não havendo esclarecimento após sete dias, o usuário deve encaminhar a dúvida por correspondência eletrônica ao CPDP no endereço cpdp@vitoria.es.gov.br.

Seção II. Gestão de Incidentes

Art. 19. Todos os usuários devem comunicar quaisquer incidentes de segurança ocorridos ou prováveis de ocorrerem, através da ferramenta ***servicedesk*** como um chamado de categoria **incidente**.

§ 1º Sempre que possível, o registro deve conter informações que auxiliem na análise do caso, como capturas de tela, mensagens de erro, arquivos ou quaisquer evidências disponíveis.

§ 2º Na impossibilidade do uso do sistema de chamados, o incidente deverá ser reportado por e-mail para nti@cdtiv.com.br ou diretamente à Coordenação de Tecnologia da Informação.

Art. 20. Qualquer situação que comprometa, ou possa comprometer, a confidencialidade, integridade, disponibilidade, autenticidade ou legalidade das informações sob responsabilidade da CDTIV será tratada como incidente de segurança da informação. A seguir, alguns exemplos de ocorrências classificadas como tal:

I. interrupção total ou parcial de sistemas, serviços ou aplicações;
II. uso indevido, impróprio ou não autorizado de recursos tecnológicos ou informações institucionais;
III. quebra ou falha de mecanismos de proteção e controle de segurança;
IV. extravio, furto, roubo ou perda de dispositivos, documentos, mídias ou credenciais de acesso;
V. falhas nos procedimentos de segurança física ou nos acessos ao ambiente institucional;
VI. movimentação não registrada ou inadequada de equipamentos, mídias ou documentos sensíveis;
VII. divulgação acidental ou proposital de informações classificadas como restritas ou sigilosas;
VIII. qualquer sinal ou ameaça que indique a possibilidade de um incidente ocorrer, ainda que não tenha se concretizado.

Art. 21. Caso detectada uma ocorrência que represente risco iminente ou dano potencial, e sempre que for viável, o uso dos sistemas ou equipamentos envolvidos deverá ser interrompido temporariamente, a fim de conter a propagação do incidente e reduzir prejuízos.

Art. 22. Após a identificação de um incidente, o responsável pela comunicação não deverá realizar investigações ou alterações no ambiente por iniciativa própria. A apuração e o tratamento técnico caberão aos gestores dos ativos afetados ou à equipe designada para essa finalidade.

Parágrafo único. Exceções serão permitidas apenas em situações críticas que exijam ações emergenciais, com o objetivo de impedir o agravamento da ocorrência, desde que sejam imediatamente reportadas após a intervenção.

Art. 23. Todos os usuários de recursos oferecidos pela CDTIV, incluindo os contratantes de seus serviços, devem zelar para que a instalação, configuração ou uso desses recursos, quando sob sua responsabilidade:

I. não causem incidentes de segurança que afetem tais recursos;
II. não permitam práticas abusivas que firam contratos ou que caracterizem mau uso;
III. não sejam aplicados para o cometimento de atos ilegais que infrinjam qualquer legislação em vigor;
IV. não coloquem em risco a integridade ou disponibilidade de ambientes tecnológicos da CDTIV ou de terceiros;
V. ocorrendo a incidência de quaisquer das situações acima, e dependendo de sua gravidade, a CDTIV poderá imediatamente efetuar a suspensão temporária dos serviços ou recursos disponibilizados, independentemente de aviso prévio, até que o usuário elimine a causa que motivou a suspensão.

Art. 24. A CDTIV poderá compartilhar dados com fornecedores e prestadores de serviço, os quais estarão contratualmente obrigados a cumprir com as normas de segurança da informação e proteção de dados. Em caso de incidentes de segurança originados por atos de terceiros, a CDTIV se compromete a adotar as medidas cabíveis, nos termos da legislação vigente, incluindo a comunicação às autoridades competentes e aos titulares dos dados, conforme aplicável.

Seção III. Gestão de Ativos

Art. 25. Todos os ATIVOS DE INFORMAÇÃO deverão ser inventariados, classificados, documentados e sua documentação mantida atualizada, devendo ser revista mensalmente ou sempre que ocorrerem fatos que justifiquem sua atualização.

§ 1º O inventário de ativos deve ser mantido atualizado, com revisões periódicas realizadas, no mínimo, a cada seis meses ou sempre que houver alterações significativas nos ativos ou em seus atributos.

Art. 26. É responsabilidade do usuário zelar pelos equipamentos sob sua guarda, mantendo-os em boas condições de uso, evitando danos físicos e prevenindo a ingestão de alimentos e bebidas nas proximidades, a fim de preservar sua integridade e funcionamento.

Art. 27. O acesso às estações de trabalho deve ser realizado mediante autenticação individual, utilizando credenciais fornecidas pela CDTIV.

§ 1º Os usuários devem bloquear suas estações de trabalho sempre que se ausentarem, mesmo que por curtos períodos, para prevenir acessos não autorizados.

§ 2º As credenciais de acesso são pessoais, confidenciais e intransferíveis; cada usuário é responsável por todas as atividades realizadas com suas credenciais.

Art. 28. Os servidores de arquivos e estações de trabalho serão protegidos com:

I. proteção de tela com ativação automática e bloqueio da estação ou através de desconexão quando o usuário necessitar afastar-se do computador;
II. software de detecção e reparo contra software ou código malicioso, com atualização frequente;
III. programação para bloqueio em caso de inatividade após 15 minutos, e desligamento às 22:00 horas diariamente.

Parágrafo único. As configurações padrão de segurança para estações de trabalho e servidores serão estabelecidas e revisadas periodicamente pelo Coordenação de Tecnologia da Informação, alinhadas às melhores práticas e normas vigentes.

Art. 29. A CDTIV não se responsabiliza por equipamentos de propriedade particular utilizados para fins corporativos.

§ 1º O uso de equipamentos particulares para atividades da CDTIV deve ser previamente autorizado e seguir as diretrizes estabelecidas pela Política de Uso de Dispositivos Pessoais.

§ 2º Equipamentos de propriedade particular sem autorização justificada não poderão acessar a rede corporativa.

Art. 30. Todas as estações de trabalho da CDTIV devem estar integradas ao sistema central de gerenciamento de usuários e dispositivos da empresa (*Active Directory*), garantindo controle adequado de acessos e aplicação das políticas de segurança.

Art. 31. Documentos essenciais para as atividades corporativas devem ser armazenados nos servidores de rede da CDTIV.

§ 1º Arquivos armazenados localmente em estações de trabalho não são considerados para fins de backup institucional e, portanto, não possuem garantia de recuperação em caso de perda ou falha do equipamento.

§ 2º É responsabilidade dos usuários assegurar que os documentos estejam devidamente armazenados nos servidores designados pela CDTIV.

Art. 32. Não é permitido o armazenamento de arquivos pessoais, como fotos, músicas, vídeos ou quaisquer arquivos que excedam 1 GB, nos servidores de rede ou em serviços de armazenamento em nuvem corporativos.

§ 1º Arquivos que não atendam a essa diretriz poderão ser removidos dos sistemas corporativos sem aviso prévio ao usuário, exceto em casos previamente autorizados pela Coordenação de Tecnologia da Informação.

§ 2º Solicitações de exceção devem ser formalizadas pelo usuário e estarão sujeitas à avaliação e aprovação da Coordenação de Tecnologia da Informação, considerando a relevância e a necessidade do armazenamento do arquivo em questão.

Seção IV. Controles de Acesso

Art. 33. O acesso aos sistemas, dados e recursos de tecnologia da informação e comunicação da CDTIV é controlado e concedido com base no princípio do menor privilégio, garantindo que cada usuário possua apenas as permissões estritamente necessárias para o desempenho de suas atribuições funcionais.

Art. 34. A identificação e autenticação dos usuários nos sistemas e redes da CDTIV são realizadas por meio de contas de acesso individuais, nominais e intransferíveis. É expressamente vedado o compartilhamento de contas ou credenciais de acesso.

Art. 35. A solicitação para criação, alteração ou remoção de contas de acesso e permissões deve ser formalizada pelo gestor imediato do usuário, através do ***servicedesk***, contendo:

I. identificação completa do usuário (nome e matrícula, se aplicável);
II. justificativa clara da necessidade do acesso ou da alteração/remoção;
III. especificação detalhada dos sistemas, recursos ou níveis de permissão requeridos ou a serem modificados/removidos;
IV. período de validade do acesso, quando aplicável (ex: para contas temporárias).

Art. 36. A ativação de novas contas de acesso está condicionada à assinatura, pelo usuário, do Termo de Responsabilidade e Confidencialidade, formalizando sua ciência e concordância com esta Política e demais normas de segurança da informação da CDTIV.

Art. 37. Contas de acesso para usuários temporários, como prestadores de serviço, consultores ou estagiários, devem:

I. ser solicitadas pelo gestor do contrato ou supervisor responsável na CDTIV;
II. possuir prazo de validade estritamente vinculado ao período contratual ou de estágio, sendo automaticamente bloqueadas ou removidas após o término;
III. ter suas permissões limitadas às necessidades específicas do serviço ou atividade a ser desempenhada;
IV. ser gerenciadas e monitoradas pela CDTIV, preferencialmente em unidades organizacionais ou grupos segregados das contas permanentes.

Art. 38. É responsabilidade do gestor imediato solicitar prontamente à CDTIV, através do ***servicedesk***:

I. a remoção ou bloqueio de contas e acessos de usuários que se desliguem da CDTIV (exoneração, demissão, término de contrato/estágio) na data do desligamento;
II. a alteração de permissões em caso de mudança de função ou setor do usuário, adequando os acessos às novas atribuições;
III. a revisão periódica dos acessos concedidos à sua equipe, validando a necessidade e adequação das permissões existentes.

Art. 39. As senhas de acesso são credenciais pessoais, confidenciais e intransferíveis, devendo atender aos seguintes requisitos mínimos estabelecidos pela CDTIV:

I. comprimento mínimo de 8 (oito) caracteres;
II. complexidade, exigindo a combinação de caracteres de diferentes grupos (letras maiúsculas, letras minúsculas, números e símbolos);
III. proibição de uso de informações pessoais (nomes, datas, documentos), palavras comuns, sequências ou repetições óbvias;
IV. verificação contra bases de senhas comprometidas conhecidas;
V. troca obrigatória no primeiro acesso;
VI. expiração periódica a cada 90 (noventa) dias;
VII. não reutilização das últimas 8 (oito) senhas utilizadas.

Art. 40. É vedado ao usuário anotar senhas em locais de fácil acesso, compartilhá-las por qualquer meio (telefone, e-mail, mensagem) ou armazená-las de forma insegura.

Art. 41. A CDTIV poderá implementar a exigência de Autenticação Multifator (MFA) para acesso a determinados sistemas, informações classificadas, acesso remoto ou contas com privilégios elevados, conforme análise de risco e normatização específica.

Art. 42. A conta de acesso será automaticamente bloqueada após 5 (cinco) tentativas consecutivas de autenticação inválida. O desbloqueio deverá ser solicitado pelo usuário à Coordenação de Tecnologia da Informação, mediante confirmação de identidade.

Art. 43. Contas de acesso que permanecerem inativas por um período superior a 45 (quarenta e cinco) dias corridos poderão ser bloqueadas pela CDTIV. A reativação dependerá de solicitação formal do usuário ou gestor, sujeita à análise da CDTIV.

Art. 44. Contas com privilégios administrativos ou de acesso a funções críticas do sistema devem seguir controles adicionais, definidos em norma específica pela CDTIV, incluindo, mas não se limitando a:

I. concessão restrita e justificada;
II. uso de contas separadas para atividades administrativas e atividades rotineiras;
III. monitoramento rigoroso de suas atividades;
IV. exigência de MFA;
V. gerenciamento seguro de senhas, preferencialmente através de cofre de senhas (*password vault*).

Art. 45. O acesso remoto à rede e aos sistemas corporativos da CDTIV, quando autorizado, deve ser realizado exclusivamente por meio de canais seguros e homologados pela CDTIV, como Redes Privadas Virtuais (VPN), e pode estar sujeito à exigência de MFA e à verificação das condições de segurança do dispositivo utilizado para o acesso.

Art. 46. Todas as tentativas de acesso, bem como as atividades realizadas nos sistemas e redes da CDTIV, são passíveis de registro (logs) para fins de auditoria, segurança, conformidade e investigação de incidentes. Tentativas de acesso não autorizado serão investigadas.

Art. 47. O usuário é o único responsável por todas as ações realizadas por meio de sua conta de acesso. O uso indevido dos recursos da CDTIV ou a violação desta Política sujeitará o usuário às sanções disciplinares, administrativas, cíveis e penais cabíveis, conforme legislação vigente e normativos internos.

Art. 48. Em caso de suspeita de comprometimento de sua conta ou senha, o usuário deve notificar imediatamente a CDTIV através dos canais oficiais.

Seção V. Acesso à Internet

Art. 49. O acesso à internet por meio da infraestrutura da CDTIV é destinado exclusivamente ao desempenho de atividades institucionais, sendo vedado seu uso para fins pessoais ou não relacionados às atribuições profissionais.

Art. 50. Todas as contas de acesso à internet serão nominativas e vinculadas às credenciais de rede da CDTIV, responsabilizando o titular por sua utilização.

I. os registros de acesso à internet poderão ser auditados para fins de segurança e conformidade;
II. é expressamente proibido utilizar o acesso à internet para atividades que violem legislações vigentes ou políticas institucionais.

Art. 51. O usuário deve cessar imediatamente o acesso a sites com conteúdo inadequado ou restrito, mesmo que tenham sido acessados inadvertidamente.

Art. 52. São consideradas práticas inaceitáveis no uso da internet:

I. acesso a sites de proxy ou serviços que contornem restrições de rede;
II. participação em jogos eletrônicos, inclusive online;

III. utilização de aplicações P2P (*peer-to-peer* ou ponto a ponto) de compartilhamento de arquivos ou similares, exemplos: *BitTorrent* ou *uTorrent*;
IV. distribuição ou compartilhamento de software ou conteúdo não autorizado;
V. disseminação de códigos maliciosos, como vírus, *worms* ou *trojans*.

Seção VI. E-mail Corporativo

Art. 53. O serviço de e-mail corporativo da CDTIV é destinado exclusivamente à comunicação relacionada às atividades institucionais, sendo vedado seu uso para fins pessoais ou não relacionados às atribuições profissionais.

Art. 54. O uso do e-mail corporativo é pessoal e intransferível, sendo o titular da conta responsável por todas as mensagens enviadas a partir de seu endereço eletrônico.

§ 1º Nos casos de contas de e-mail compartilhadas ou setoriais, a responsabilidade pelas mensagens enviadas recairá sobre todos servidores que utilizam a conta, conforme registro formalizado junto à CDTIV.

§ 2º A criação de contas de e-mail setoriais deverá ser solicitada pelo chefe imediato da unidade, mediante justificativa formal e aprovação da Coordenação de Tecnologia da Informação.

Art. 55. O conteúdo das mensagens de e-mail é considerado confidencial, estando o acesso restrito ao remetente e ao(s) destinatário(s), salvo em casos de auditoria, investigação de incidentes de segurança ou por determinação legal, devidamente autorizados pela autoridade competente.

Parágrafo único. O acesso não autorizado a mensagens de e-mail alheias constitui violação das normas institucionais e poderá sujeitar o infrator às sanções administrativas, civis e penais cabíveis.

Art. 56. As mensagens de e-mail devem ser redigidas em linguagem clara, objetiva e profissional, respeitando as normas gramaticais da língua portuguesa e os princípios éticos da administração pública, de forma a preservar a imagem institucional da CDTIV.

Art. 57. Os usuários devem estar atentos à origem e ao conteúdo das mensagens recebidas, evitando abrir anexos ou clicar em links de remetentes desconhecidos ou suspeitos.

Parágrafo único. Em caso de recebimento de mensagens suspeitas ou que possam representar risco à segurança da informação, o usuário deverá encaminhá-las imediatamente à Coordenação de Tecnologia da Informação para análise e providências.

Seção VII. Dispositivos Móveis

Art. 58. A utilização de dispositivos móveis para acesso a informações e recursos da CDTIV deve priorizar a proteção da confidencialidade, integridade e disponibilidade dos dados institucionais, observando-se as diretrizes estabelecidas nesta Política.

Art. 59. Ficam estabelecidos os seguintes requisitos mínimos de segurança, aplicáveis a todos os dispositivos móveis, sejam eles corporativos ou de propriedade particular, que acessem ou armazenem informações da CDTIV:

I. é vedada a instalação de aplicativos de fontes não confiáveis ou que solicitem permissões excessivas e não justificadas para sua funcionalidade;
II. é obrigatório a configuração e uso de mecanismo de bloqueio de tela (senha, PIN, padrão ou biometria), com complexidade adequada e ativação automática após curto período de inatividade, conforme orientação da CDTIV.

Art. 60. Os dispositivos móveis fornecidos pela CDTIV (corporativos) seguirão as seguintes diretrizes adicionais:

I. serão devidamente registrados e inventariados pela CDTIV, vinculando o equipamento ao usuário responsável;
II. a configuração inicial, incluindo mecanismos de segurança como criptografia de armazenamento e antivírus (quando aplicável), será realizada ou homologada pela CDTIV;
III. destinam-se ao uso exclusivo do usuário designado, que assume a responsabilidade por sua guarda e correto manuseio;
IV. a instalação de novos aplicativos ou recursos que não façam parte da configuração padrão homologada pela CDTIV dependerá de análise e autorização prévia da Coordenação de Tecnologia da Informação;
V. a CDTIV implementará mecanismos para autenticação segura, autorização e registro de logs de acesso do dispositivo e do usuário aos recursos da rede corporativa;

VI. a CDTIV reserva-se o direito de monitorar o uso do dispositivo para fins de segurança, conformidade e auditoria, respeitando a legislação vigente, bem como de aplicar remotamente políticas de segurança, bloqueio ou limpeza de dados (*wipe*) em caso de perda, roubo, desligamento do usuário ou comprometimento de segurança identificado;
VII. o usuário será formalmente orientado sobre seus deveres e responsabilidades mediante assinatura de Termo de Uso e Responsabilidade específico.

Art. 61. A utilização de dispositivos móveis de propriedade particular (BYOD - *Bring Your Own Device*) para acesso a recursos corporativos obedecerá às seguintes regras:

I. o acesso a recursos corporativos por meio de dispositivo particular está condicionado à expressa autorização da chefia imediata e da CDTIV, mediante solicitação formal do usuário;
II. a solicitação deverá justificar a necessidade de acesso e especificar os recursos demandados, estando sujeita à análise de viabilidade e risco pela CDTIV;
III. o dispositivo particular deverá atender integralmente aos requisitos mínimos de segurança estabelecidos no Art. 59 desta Política.
IV. a CDTIV poderá exigir a instalação de aplicativos ou perfis de gerenciamento (MDM/MAM) para criar um ambiente seguro e segregado para os dados e aplicações corporativas no dispositivo particular.
V. o usuário proprietário é responsável pela segurança geral do seu dispositivo, incluindo a proteção de seus dados pessoais. A CDTIV não se responsabiliza por perda de dados pessoais, custos de manutenção ou eventuais danos ao equipamento particular.
VI. a CDTIV implementará mecanismos de autenticação, autorização e registro de acesso para o dispositivo e usuário particulares.
VII. em caso de desligamento do usuário, perda, roubo ou suspeita de comprometimento da segurança do dispositivo particular, a CDTIV poderá remover remotamente o acesso, os dados e as aplicações corporativas. Dependendo da solução de gerenciamento implementada e da gravidade do risco, poderá ser necessária a limpeza completa (*wipe*) do dispositivo, da qual o usuário estará ciente ao solicitar o acesso.
VIII. o usuário será orientado sobre os procedimentos e riscos associados ao uso de dispositivo particular para fins corporativos, formalizando sua ciência e concordância mediante assinatura de Termo de Uso e Responsabilidade.

Art. 62. Em caso de furto, roubo, perda, extravio ou dano a um dispositivo móvel (corporativo ou particular com acesso a dados da CDTIV), é responsabilidade do usuário:

I. notificar imediatamente sua chefia imediata e a CDTIV, fornecendo todas as informações relevantes sobre o ocorrido;
II. registrar boletim de ocorrência policial nos casos de furto ou roubo, encaminhando cópia à CDTIV assim que possível;
III. cooperar integralmente com a CDTIV nas ações necessárias para tentativa de localização, bloqueio de acesso e/ou limpeza remota dos dados corporativos contidos no dispositivo.

CAPÍTULO VIII – GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 63. A estrutura de Gestão de Segurança da Informação da CDTIV é composta por:

I. Diretoria Executiva;
II. Coordenação de Tecnologia da Informação;
III. Encarregado pelo Tratamento de Dados Pessoais; e
IV. Usuários.

Seção I. Diretoria Executiva

Art. 64. Compete à Diretoria Executiva:

I. fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação da CDTIV, bem como com o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados; e
II. formalizar e aprovar a PSI da CDTIV, bem como suas alterações e atualizações.

Seção II. Coordenação de Tecnologia da Informação

Art. 65. Compete à Coordenação de Tecnologia da Informação:

I. planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução;

II. coordenar a elaboração da PSI e das normas internas de segurança da informação da Companhia, observadas a legislação vigente e as melhores práticas sobre o tema;
III. assessorar a Diretoria Executiva na implementação da Política de Segurança da Informação;
IV. estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;
V. promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão;
VI. acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação.

Seção III. Encarregado pelo Tratamento dos Dados Pessoais

Art. 66. Compete ao Encarregado pelo Tratamento dos Dados Pessoais, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD) e demais normativos e orientações emitidas pela Autoridade Nacional de Proteção de Dados (ANPD), conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis.

Seção IV. Usuários

Art. 67. Compete aos Usuários conhecer, cumprir e fazer cumprir esta Política e às demais normas específicas de segurança da informação da CDTIV.

Art. 68. Todos os Usuários são responsáveis pela segurança dos ativos de informação que estejam sob a sua responsabilidade.

CAPÍTULO IX – DAS VEDAÇÕES

Art. 69. É vedada a utilização dos recursos de tecnologia da informação disponibilizados pela CDTIV para acesso, guarda e divulgação de material incompatível com ambiente do serviço, que viole direitos autorais ou que infrinja a legislação vigente.

Art. 70. É vedado utilizar os ativos de informação para constranger, assediar, prejudicar ou ameaçar qualquer pessoa.

Art. 71. É vedado fazer-se passar por outra pessoa ou camuflar sua identidade quanto utilizar os ativos de informação.

Art. 72. São vedados o uso e a instalação de recursos de tecnologia da informação que não tenham sido homologados ou adquiridos pela CDTIV.

Art. 73. É vedada a divulgação a terceiros de mecanismos de identificação, autenticação e autorização baseados em conta e senha ou certificação digital, de uso pessoal e intransferível, que são fornecidos aos usuários.

Art. 74. É vedada a exploração de eventuais vulnerabilidades, as quais devem ser comunicadas às instâncias superiores assim que identificadas.

CAPÍTULO X – PENALIDADE

Art. 75. Ações que violem a PSI poderão acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 76. Penalidades às violações desta PSI serão aplicadas conforme a gravidade do ato cometido, podendo variar de mera advertência verbal ou notificação escrita à aplicação dos sansões previstas em contratos, estatutos e outros regulamentos, além das legislações trabalhista, civil, criminal e demais leis específicas aplicáveis.

Art. 77. Nas violações passíveis de serem consideradas violação desta PSI envolvendo empregados e servidores (incluindo comissionados e servidores cedidos), caberá à Diretoria Executiva decidir pela abertura de Sindicância/PAD (Processo Administrativo Disciplinar) interno, dependendo da gravidade da violação cometida.

Art. 78. Independentemente da adoção das medidas acima, caso sejam cometidas violações consideradas delitos ou crimes perante a legislação brasileira, a CDTIV preservará as evidências e cooperará com as autoridades competentes.

CAPÍTULO XI – DISPOSIÇÕES FINAIS

Art. 79. A Coordenação de Tecnologia da Informação deve promover ações de treinamento e conscientização para que os usuários entendam suas responsabilidades e procedimentos voltados à segurança da informação e à proteção de dados.

Art. 80. A conscientização, a capacitação e a sensibilização em segurança da informação devem ser adequadas aos papéis e responsabilidades dos servidores.

Art. 81. As denúncias de violação a esta PSI podem ser comunicadas à Coordenação de Tecnologia da Informação e feitas através dos seguintes canais:

I. **E-mail:** nti@cdtiv.com.br;
II. ***Servicedesk:*** abertura chamado de categoria **incidente.**

Art. 82. O cumprimento desta PSI, bem como dos normativos que a complementam devem ser avaliados pela CDTIV periodicamente por meio de verificações de conformidade, buscando a certificação do cumprimento dos requisitos de segurança da informação e da garantia de cláusula de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

Art. 83. A não observância do disposto nesta PSI, bem como em seus instrumentos normativos correlatos, sujeita o infrator à aplicação de sanções administrativas conforme a legislação vigente, sem prejuízo das responsabilidades penal e civil, assegurados sempre aos envolvidos o contraditório e a ampla defesa.

Art. 84. Esta PSI será revisada periodicamente em prazos não superior a 2 anos, para refletir as mudanças no ambiente da CDTIV, nos riscos à segurança da informação e nas melhores práticas de segurança da informação compatíveis a realidade da Companhia.

Art. 85. Os casos omissos e as dúvidas sobre a PSI e seus documentos devem ser submetidas ao Coordenação de Tecnologia da Informação.