ITA

Inteligência
em Frotas

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Índice

1 - Introdução

2 - Princípios

3 - Valores

4 - Comitê de Ética

5 -Uso aceitável de ativos de informação da ITA por seus usuários autorizados

6 - Das Sanções e Punições

7 - Disposições Gerais

8 - Gestão da Norma

9 - Vigência e atualização

1. Introdução

A “Política de Segurança da Informação da ITA Empresa de Transportes Ltda.”, apresenta os controles internos aplicáveis à segurança e ao sigilo da Informação da instituição com o objetivo de fornecer a garantia necessária para realização de suas operações, ainda que em situações adversas.

1.1. Escopo

A Política de Segurança da Informação da ITA, aborda as boas práticas de governança, princípios e diretrizes gerais aplicáveis à segurança e ao sigilo das informações, custodiadas ou de propriedade da ITA, nos termos da lei nº 13.709, de 14 de agosto de 2018, CAPÍTULO VII, DA SEGURANÇA E DAS BOAS PRÁTICAS.

1.2. Propósito

Estabelecer diretrizes para utilização segura dos dados em processamento ou armazenados nos bancos de dados da ITA.

1.3. Público-Alvo

Este documento se destina a toda a comunidade da ITA: empregados, ex-empregados, diretores, estagiários, prestadores de serviço, visitantes e usuários externos que façam uso de algum sistema de informação da ITA, sendo de responsabilidade de cada um o seu cumprimento.

2. Princípios

A Política de Segurança da Informação da ITA está fundamentada na preservação das informações necessárias às atividades da empresa e nos seguintes princípios:

2.1. Autenticidade: garante a veracidade da autoria da informação.

2.2. Confidencialidade: somente pessoas devidamente autorizadas devem ter acesso à informação.

2.3. Integridade: somente alterações, supressões e adições autorizadas devem ser realizadas nas informações.

2.4. Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.

2.5. Legalidade: o uso da informação deve estar de acordo com as leis, regulamentos, licenças e contratos em vigência.

3. Valores

3.1. Segurança Focada na Instituição: Garantir a segurança da informação tanto aos sistemas no ambiente de computação, quanto aos meios convencionais de processamento, comunicação e armazenamento em papel.

3.2. Informação é patrimônio: Considerar que toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela ITA é patrimônio da instituição e deve ser protegida quanto aos aspectos de confidencialidade, autenticidade, integridade e disponibilidade.

3.3. Proteção compatível com os riscos: Dimensionar e aplicar os investimentos necessários em medidas de segurança, segundo o valor do ativo que está sendo protegido e de acordo com a identificação de riscos de potenciais prejuízos ao negócio, à atividade fim e aos objetivos institucionais.

3.4. Tratamento conforme a classificação: Todas as informações devem ser adequadamente armazenadas e protegidas quanto ao uso e acesso, conforme definido em sua classificação de segurança.

3.5. Responsabilização baseada na credencial: Responsabilizar, com base no uso da credencial, que se caracteriza por ser pessoal e intransferível, qualificando aquele que se encontra formalmente associado a ela como responsável por todas as atividades desenvolvidas em seu uso.

3.6. Utilização restrita às atividades: Administrar o acesso e o uso da informação e dos ativos de informação de acordo com as atribuições necessárias para o cumprimento das atividades institucionais. Qualquer outra forma de uso necessitará de prévia autorização.

3.7. Utilização orientada à segurança: Permitir somente o uso de ativos de informação ou ativos de processamento autorizados pelos gestores, sempre se atentando que estes estejam identificados, protegidos, inventariados e de acordo com a legislação vigente.

3.8. Autorização definida pelos gestores: Definir e cancelar acessos aos recursos e aos locais restritos com base na solicitação dos gestores de cada área, que também são responsáveis pelos ativos disponibilizados para uso.

3.9. Segregação de funções: Segregar a administração e execução de funções ou áreas de responsabilidade críticas para o negócio, evitando o controle de um processo na sua totalidade, visando à redução do risco de mau uso acidental ou deliberado.

3.10. Educação e Capacitação: Promover continuamente ações educativas e de capacitação sobre segurança da informação ao público-alvo para que realizem suas atividades na instituição de forma segura, utilizando procedimentos que minimizem os riscos e que possibilitem o uso correto dos ativos e ferramentas de informação.

3.11. Continuidade aplicada aos serviços: Planejar e definir estratégias para reduzir, a um nível aceitável, a possibilidade de interrupção causada por desastres ou falhas nos recursos que suportam os processos de trabalho.

3.12. Notificação imediata de incidentes de segurança: Notificar todos os incidentes de segurança ao Comitê de Ética para encaminhamento dos processos necessários à apuração de responsabilidades.

4. Comitê de Ética

As atribuições e responsabilidades pela execução da Política de Segurança da Informação da ITA serão confiadas ao "Comitê de Ética", que será composto por 5 (cinco) membros designados pelo presidente da empresa e aprovados pelo Conselho.

4.1. Das Responsabilidades do Comitê de Ética

4.1.1. Avaliar, aprovar ou negar solicitações para uso de dispositivos pessoais no ambiente corporativo;

4.1.2. Criar termos de consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

4.1.3. Estabelecer as regras de proteção dos ativos da ITA;

4.1.4. Revisar frequentemente as regras de proteção estabelecidas;

4.1.5. Restringir e controlar o acesso e privilégios de usuários remotos e externos;

4.1.6. Executar as regras de proteção estabelecidas por esta Política;

4.1.7. Detectar, identificar, registrar e comunicar à presidência da empresa violações ou tentativas de acessos não autorizados;

4.1.8. Definir e aplicar, para cada usuário de tecnologia da informação, restrições de acesso à rede, como horário e dia autorizados, entre outras;

4.1.9. Limitar ao período da contratação o prazo de validade das contas de prestadores de serviço;

4.1.10. Solicitar e gerir, quando necessário, auditoria para verificação de acessos indevidos;

4.1.11. Solicitar, quando julgar necessário, o bloqueio de chaves de acesso de usuários;

4.1.12. Excluir ou desabilitar as contas inativas;

4.1.13. Fornecer senhas de contas privilegiadas somente aos usuários que necessitem efetivamente de tais privilégios, mantendo-se o devido registro e controle.

4.2. A comunicação com o Comitê de Ética deve ser diretamente encaminhada ao Analista de Conformidade.

5. Uso aceitável de ativos de informação da ITA por seus usuários autorizados

5.1. Uso de equipamentos de propriedade da ITA

5.1.1. A ITA fornece para seus usuários equipamentos para o desempenho exclusivamente de suas atividades profissionais;

5.1.2. A alteração e a manutenção de qualquer equipamento de propriedade da ITA é uma atribuição específica da Assessoria de Tecnologia da Informação que, a seu critério exclusivo, poderá delegar formalmente outro responsável. Demais usuários são expressamente proibidos de realizar qualquer tipo de manutenção ou modificação nos equipamentos;

5.1.3. Os equipamentos da ITA devem ser utilizados com cuidado visando garantir sua preservação e seu funcionamento adequado;

5.1.4. Computadores de mesa (desktops) ou móveis (notebooks) devem ser desligados no final do expediente ou sempre que um usuário estiver ausente por um período prolongado, excetuando-se quando existir uma justificativa plausível em virtude de atividades de trabalho;

5.1.5. A desconexão (log off) da rede deverá ser efetuada nos casos em que o usuário não for mais utilizar o equipamento ou venha a ausentar-se de seu ambiente de trabalho;

5.1.6. O bloqueio de tela protegido por senha deverá ser ativado quando o usuário se afastar do computador de mesa ou móvel que esteja utilizando;

5.1.7. Ao final do contrato de trabalho, os equipamentos disponibilizados para a execução de atividades profissionais devem ser devolvidos em estado de conservação adequado quando no desligamento ou término da relação do colaborador com a ITA;

5.1.8. Qualquer dano aos equipamentos da ITA será devidamente analisado pela Assessoria de Tecnologia da Informação. Havendo a constatação de que tal dano decorreu de ação direta ou omissão do usuário, caberá a ITA exercer seu direito de reparação ao prejuízo, através da tomada das medidas cabíveis;

5.1.9. A seu critério exclusivo a ITA poderá permitir a utilização de equipamento particular para o desempenho de atividades profissionais, devendo os mesmos estar adequados aos requisitos e controles de segurança adotados pela empresa e com a devida autorização formal pela Assessoria de Tecnologia da Informação;

5.1.10. Quando ocorrer movimentação interna dos equipamentos ativos, a Assessoria de Tecnologia da Informação garantirá que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

5.2. Dos Dispositivos de Armazenamento Removível

5.2.1. A ITA poderá, a seu critério exclusivo, fornecer a seus usuários dispositivos de armazenamento removível exclusivamente para a execução de suas atividades profissionais, devendo ser observadas as seguintes orientações:

5.2.1.1. O usuário é o responsável direto pela segurança física e lógica dos dispositivos móveis sob sua guarda;

5.2.1.2. Em caso de perda ou furto de um dispositivo de armazenamento removível, o usuário deve comunicar imediatamente a Assessoria de Tecnologia da Informação.

5.3. Armazenamento remoto (nuvem)

5.3.1. A ITA disponibiliza para seus usuários espaço para armazenamento remoto de arquivos na nuvem, através de sua solução corporativa.

5.3.2. A ITA requer que seus colaboradores não arquivem documentos que possuem informações de clientes, funcionários, terceiros e do negócio em áreas de uso público, evitando que informações restritas e confidenciais sejam disponibilizadas e acessadas de forma indevida.

5.3.2.1. Informações Internas: São informações que estão disponíveis aos colaboradores por meio das ferramentas aprovadas, com armazenamento interno, em servidores da ITA ou terceiros autorizados (na nuvem, por exemplo). Qualquer Informação classificada como "INTERNA" não poderá ser encaminhada, divulgada ou publicada em quaisquer meios para terceiros não autorizados, devendo a sua disponibilização ser restrita ao ambiente de trabalho e uso limitado aos colaboradores ou terceiros, que realmente necessitem ter acesso a tais Informações.

5.3.2.2. Informações Restritas: Normalmente são Informações de uma determinada área que não deve ser acessada por outros setores da empresa, por exemplo, os documentos do setor de RH ou departamento financeiro da empresa.

5.3.2.3. Informações Confidenciais: Referidas informações deverão ser mantidas em arquivos físicos ou eletrônicos com níveis de segurança compatíveis com a relevância da Informação. A transmissão de arquivos confidenciais só deverá ser feita utilizando meios de transmissão seguras, para as partes previamente autorizadas, com contrato de sigilo claro e dentro da validade, sejam as partes: funcionários, colaboradores, associados, fornecedores ou qualquer tipo de parceiro de negócios que precisam: criar, armazenar ou processar qualquer tipo de Informação CONFIDENCIAL.

5.4. Identificação digital

5.4.1. A ITA poderá, a seu critério exclusivo, fornecer certificados digitais a usuários para a execução de atividades profissionais específicas, devendo ser observadas as seguintes diretrizes:

5.4.1.1. Cabe exclusivamente ao usuário a conservação de seu certificado digital, independentemente do equipamento que o suporte, bem como de qualquer tipo de senha ou meio de autenticação relacionado ao mesmo.

5.3.2. A ITA requer que seus colaboradores não arquivem documentos que possuem informações de clientes, funcionários, terceiros e do negócio em áreas de uso público, evitando que informações restritas e confidenciais sejam disponibilizadas e acessadas de forma indevida.

5.4.1.2. O usuário deverá informar a Assessoria de Tecnologia da Informação sobre quaisquer eventos ou suspeitas relativas ao comprometimento de sua senha e/ou o uso indevido de seu certificado digital;

5.4.1.3. O usuário desligado ou em processo de desligamento terá o certificado digital expedido pela ITA imediatamente revogado.

5.5. Equipamentos de impressão e de fotocópias

5.5.1. O uso de equipamentos de impressão e fotocopiadoras deve ser feito exclusivamente para a impressão/reprodução de documentos que sejam de interesse da ITA ou que estejam relacionados com o desempenho das atividades profissionais do usuário.

5.5.2. O usuário deve observar as seguintes disposições específicas quanto ao uso de equipamentos de impressão e fotocópia:

5.5.2.1. O usuário deve retirar imediatamente da impressora ou fotocopiadora os documentos que tenha solicitado a impressão, transmissão ou cópia que contenham informações da ITA, classificadas como de uso interno ou confidencial;

5.5.2.2. A impressão ou cópia de documento em meio físico deve ser limitada à quantidade exata necessária para a tarefa determinada;

5.5.2.3. Não será admissível, em nenhuma hipótese, o reaproveitamento de páginas já impressas e contendo informações classificadas como restritas ou confidenciais, devendo as mesmas ser descartadas de acordo com os procedimentos adotados pela ITA.

5.6. Da Segurança física

5.6.1. As instalações de processamento das informações da ITA serão mantidas em áreas seguras, cujo perímetro é fisicamente isolado contra o acesso não autorizado, os danos e quaisquer interferências de origem humana ou natural.

5.6.2. O usuário deve observar as seguintes disposições específicas quanto à segurança física:

5.6.2.1. Crachás de identificação, inclusive temporários, são pessoais e intransferíveis. Sob nenhuma circunstância será permitido o seu compartilhamento;

5.6.2.2. Enquanto em áreas sensíveis, os colaboradores devem portar crachás de identificação que exibam claramente seu nome e fotografia. Terceiros autorizados devem portar crachás temporários identificando claramente que os mesmos não são colaboradores da ITA;

5.6.2.3. Excetuando-se quando formalmente autorizado, terceiros nunca devem ser deixados sozinhos em áreas sensíveis;

5.6.2.4. É proibida qualquer tentativa de se obter ou permitir o acesso a indivíduos não autorizados a áreas sensíveis da ITA;

5.6.2.5. É resguardado a ITA o direito de inspecionar malas, maletas, mochilas e similares, assim como quaisquer equipamentos, incluindo dispositivos móveis, antes de permitir a entrada ou saída de colaboradores ou terceiros de áreas sensíveis;

5.6.2.6. É resguardado a ITA o direito de monitorar seus ambientes físicos. Para isso será utilizado sistema de circuito fechado de televisão em áreas comuns. As imagens obtidas serão armazenadas e protegidas contra qualquer tipo de manipulação indevida;

5.6.2.7. Os documentos classificados como uso interno, restrito ou confidencial, após manuseados, não deverão ser deixados expostos em cima de mesas, assim, ao se ausentar cabe ao usuário o dever de mantê-los guardados ou descartá-los de acordo com os procedimentos determinados;

5.6.2.8. Não é permitido consumir qualquer tipo de alimento, bebida ou fumar em áreas identificadas como sensíveis.

5.7. Do Acesso à internet fornecido pela ITA Empresa de Transportes Ltda.

5.7.1. A ITA fornece acesso à Internet aos seus usuários autorizados, conforme as necessidades inerentes ao desempenho de suas atividades profissionais;

5.7.2. O acesso à internet pode ser fornecido tanto através da rede corporativa da ITA, quanto através da disponibilização de serviços de internet móvel, prestados por terceiros, contratados pela ITA;

5.7.3. Toda informação que é acessada, transmitida, recebida ou produzida através do acesso à internet fornecido pela ITA está sujeita a monitoramento, não havendo por parte do usuário qualquer expectativa de privacidade;

5.7.4. Durante o monitoramento do acesso à internet, a ITA se resguarda o direito de, sem qualquer notificação ou aviso, interceptar, registrar, ler, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais, toda informação trafegada, seja originada de sua rede interna e destinada a redes externas ou o contrário;

5.7.5. Durante o acesso à Internet fornecido pela ITA não será permitido o download, o upload, a inclusão, a disponibilização, a visualização, a edição, a instalação, o armazenamento ou a cópia de qualquer conteúdo relacionado expressa ou subjetivamente, direta ou indiretamente, com:

5.7.5.1. Qualquer espécie de exploração sexual;

5.7.5.2. Qualquer forma de conteúdo adulto, erotismo, pornografia;

5.7.5.3. Qualquer tipo de Pornografia infantil;

5.7.5.4. Qualquer forma de ameaça, chantagem e assédio moral ou sexual;

5.7.5.5. Qualquer ato calunioso, difamatório, infamante, vexatório, aviltante ou atentatório à moral e aos bons costumes da sociedade;

5.7.5.6. Preconceito baseado em cor, sexo, orientação sexual, raça, origem, condição social, crença, religião, deficiências e necessidades especiais;

5.7.5.7. Incentivo ao consumo de bebidas alcoólicas, fumo e substâncias entorpecentes, sejam essas lícitas ou não;

5.7.5.8. A prática e/ou a incitação de crimes ou contravenções penais;

5.7.5.9. A prática de propaganda política nacional ou internacional;

5.7.5.10. A prática de quaisquer atividades comerciais desleais;

5.7.5.11. O desrespeito à imagem ou aos direitos de propriedade intelectual e industrial da ITA;

5.7.5.12. A disseminação de códigos maliciosos e ameaças virtuais;

5.7.5.13. Tentativa de expor a infraestrutura computacional da ITA a ameaças virtuais;

5.7.5.14. Divulgação não autorizada de qualquer informação da ITA classificada como confidencial ou de uso interno;

5.7.5.15. Uso de sites ou serviços que busquem contornar controles de acesso à internet.

5.8. Do Comportamento corporativo em mídias e redes sociais

5.8.1. A publicação de conteúdo referente à ITA em mídias e redes sociais é feita por setores e usuários que possuem essa responsabilidade específica, sendo os demais usuários proibidos de publicar qualquer tipo de informação em nome da instituição.

5.8.2. Quando no uso de suas mídias e redes sociais particulares, empregados, prestadores de serviço e terceiros contratados devem observar as seguintes restrições:

5.8.2.1. Não é permitido o uso da logomarca, bem como de qualquer parte da identidade visual da ITA sem autorização prévia e expressa;

5.8.2.2. Não é permitida a criação, participação ou interação com quaisquer perfis, comunidades, grupos, tópicos de discussão e afins que empreguem o nome, marca ou outros sinais distintivos da ITA, excetuando-se os canais oficiais da instituição;

5.8.2.3. Não é permitida a publicação de conteúdo ou comentários diretamente relacionados à ITA, seus trabalhadores, terceiros contratados e prestadores de serviço;

5.8.2.4. Não é permitida a publicação de qualquer tipo de imagem, foto, vídeo, áudio relacionado ao ambiente corporativo da ITA sem a expressa autorização da instituição, excetuando-se material divulgado em canais oficiais.

6. Das Sanções e Punições

6.1. O público-alvo desta política está sujeito às regras da mesma, devendo observar integralmente suas disposições. A inobservância dessas regras acarretará apuração de responsabilidades, na forma da legislação em vigor, podendo haver responsabilização penal, civil e/ou administrativa, sem prejuízo da rescisão do contrato de trabalho e/ou qualquer outro contrato de relacionamento de prestação de serviço entre o colaborador, associado, consultor, assim como qualquer entidade com relação contratual direta ou indireta com a ITA.

6.2. Ao público-alvo não é dado o direito de desconhecimento desta política, devendo o mesmo seguir rigorosamente o estabelecido nas normas de segurança.

6.3. É dever de todos os trabalhadores da ITA informar e reportar inconsistências em procedimentos e práticas definidas no presente documento, seja para seu superior imediato ou para o Analista de Conformidade.

7. Disposições Gerais

7.1. Qualquer tipo de dúvida sobre a Política de Segurança da Informação da ITA e seus documentos deve ser imediatamente esclarecida junto ao Analista de Conformidade.

7.2. Casos omissos, os quais não estão cobertos por esta política, deverão ser submetidos ao Comitê de Ética em exercício, para que haja apreciação e deliberação, definindo assim se o objeto será incluído ou resultará na alteração de algum ponto da política em vigência.

8. Gestão da Norma

8.1. A Norma de segurança da informação é aprovada pelo Comitê de Ética, em conjunto com a Presidência da ITA Empresa de Transportes LTDA.

8.2. A presente norma foi aprovada no dia 07/06/2022.

9. Vigência e atualização

9.1. Este documento entra em vigor a partir da data de sua publicação e deve ser revisto em caso de ocorrência de alguma das condições obrigatórias de atualização do documento.

Atualização:

Essas diretrizes foram atualizadas em 07/06/2022.
Condições obrigatórias para atualização do documento:
Surgimento ou alteração de leis e/ou regulamentações vigentes;
Mudança estratégica da instituição;
Mudança nas tecnologias utilizadas na ITA.

Comitê de Ética