POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

Patrus Transportes Ltda

N.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

PATRUS TRANSPORTES LTDA

N. 001 2021-09-30

Preâmbulo

Todas as informações que dizem respeito à Patrus são de sua exclusiva titularidade, podendo ser geridas de acordo com suas necessidades, sendo vedado seu compartilhamento por meios particulares ou com pessoas não autorizadas.

CAPÍTULO 1 – DISPOSIÇÕES GERAIS

Definições

Art. 1º No âmbito desta Política de Segurança da Informação, os seguintes termos, expressões e palavras são empregados, no singular ou no plural, de acordo com as definições ora estabelecidas:

I – PATRUS: empresa de soluções em transporte de carga fracionada B2B e B2C, inscrita no CNPJ sob o nº 17.463.456/0035-30, com sede no município de Contagem, estado de Minas Gerais, na Rua José Barbosa Melo, 145, Bairro Cinco e nome fantasia PATRUS.

II – Colaborador: empregados e os estagiários da PATRUS por ela diretamente contratados com base na legislação trabalhista;

III – Bolsista: pessoa física recebe uma bolsa em razão de uma atividade que desenvolve, vinculada a um Plano de Ação e relacionada a um convênio/projeto mantido por uma Entidade Concedente;

IV – Prestador de Serviço: pessoa física ou jurídica que, por força de contrato firmado com esse objetivo, presta serviços de qualquer natureza, a qualquer das unidades da PATRUS**;**

V – Fornecedor: pessoa física ou jurídica que, por força de contrato firmado com este objetivo, fornece bens ou produtos de qualquer natureza, a qualquer das unidades da **PATRUS;**

VI – Recursos de Tecnologia da Informação (TI): conjunto de bens ou recursos materiais ou imateriais que integra o sistema de tecnologia da informação de qualquer das unidades da **PATRUS**, tais como computadores de mesa (*desktop*) e seus acessórios, computadores portáteis (tais como *notebooks, netbooks, laptops, palmtops, tablets*), servidores de rede, redes

de dados, redes de telefonia, redes de conexão à Internet, Sistemas Corporativos, *softwares*, Dispositivos de Armazenamento, *scanners*, impressoras, aparelhos de áudio e videoconferência, Mídias Sociais e manuais técnicos, bem como quaisquer outros recursos tecnológicos utilizados para a execução das atividades profissionais;

VII – Unidade: toda edificação que integra a **PATRUS,** incluindo hospitais e demais sedes administrativas;

VIII – Sistemas Corporativos: todos os sistemas e aplicativos utilizados, no âmbito da **PATRUS**, para o exercício das atividades profissionais: rede corporativa, Correio Eletrônico Corporativo, Soul MV, TOTVS, Interact, CareStream, TrackSale, dentre outros;

IX – Correio Eletrônico Corporativo (*e-mail* corporativo): endereço de e-mail corporativo adotado pela **PATRUS**, atribuído pela Gerência de Gestão da Informação;

X – Conta de Usuário: conta utilizada pelos Usuários para acesso aos Sistemas Corporativos, vinculada a um nome de *login* atribuído individualmente a cada Usuário pela Gerência de Gestão da Informação e uma senha;

XI – Setor de Tecnologia da Informação (Setor de TI): setor responsável pelo gerenciamento e administração dos Recursos de Tecnologia da Informação;

XII – Setor de Comunicação e Marketing: setor responsável pela criação de soluções de marketing que satisfaça o

público-alvo da **PATRUS**, trabalhando para que atinjam o público de maneira eficiente e direcionada;

XIII – Setor de Recursos Humanos (Setor de RH): setor responsável pela gestão de relacionamento dos colaboradores com a **PATRUS**;

XIV – Mídias Sociais: estruturas pertencentes à rede mundial de computadores que permitem o compartilhamento de informações via redes sociais, ferramentas, *wikis, blogs, microblogs*, sites de compartilhamento de vídeos, dentre outras. São exemplos de tais mídias: Facebook, Instagram, Twitter, Snapchat, Blogger, Wordpress, LinkedIn, Youtube, Wikipedia, Flickr;

XV – Mídias de Armazenamento: recursos materiais ou eletrônicos utilizados para o armazenamento de informações, incluindo dispositivos eletrônicos como fitas, discos, HDs externos (dispositivos de armazenamento magnético), *pen drives* (além de outros dispositivos que utilizam memória *flash*), CDs e DVDs (dispositivos de armazenamento óptico), bem como documentos impressos ou manuscritos;

XVI – Ativos Intangíveis: grande variedade de informações armazenadas em formato digital, compreendendo documentos, imagens, áudio, vídeo, bancos de dados e outros bens imateriais cujo conteúdo é de titularidade exclusiva da **PATRUS**;

XVII – Dados Pessoais: informações relacionadas a uma pessoa natural identificada ou identificável:

a) Tratamento de Dados Pessoais: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XVIII – Informações Estratégicas: todos os dados e informações que possuem relevância estratégica para a **PATRUS,** tais como, mas não limitados a informações financeiras, contratuais, planos de ação, dados de Colaboradores, dentre outros;

XVIX – Incidente de Segurança da Informação: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas da informação capaz de alterar ou causar a perda dos princípios básicos da informação: confidencialidade, integridade e disponibilidade;

XX – Fragilidades em Sistemas ou Serviços: vulnerabilidades encontradas em *softwares* e aplicativos que podem ser exploradas por ameaças colocando em risco a confidencialidade, disponibilidade e integridade das informações.

Objetivos e Abrangência

Art. 2º A Política de Segurança da Informação da **PATRUS** estabelece normas cujo principal objetivo é a proteção das informações armazenadas ou circulando no âmbito dos Recursos de TI, buscando seu resguardo quanto a acesso lógico não autorizado, ação de vírus de computador, erros ou omissões em sua utilização, de uso indevido, extravio ou vazamento de informações, de sabotagem, falhas de *hardware* e indisponibilidade de serviços ou informações.

Art. 3º Esta Política de Segurança da Informação está em conformidade com o Estatuto Social, Código de Ética e Conduta, Manual de Compliance e demais normas internas da **PATRUS**, com o Plano Geral de Segurança da Tecnologia da Informação (PLC-TI-001) e seus respectivos Procedimentos Operacionais-Padrão (Anexo II), bem como a legislação brasileira correlata, em especial a Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), Lei n. 12.846/2013 (Lei Anticorrupção) e a legislação trabalhista.

Art. 4º Além das normas expressamente previstas neste documento, todas aquelas nele referenciadas integram a Política de Segurança da Informação da **PATRUS**.

Art. 5º As normas constantes da Política de Segurança da Informação da **PATRUS** são aplicáveis a todas as unidades da **PATRUS**.

Art. 6º A Política de Segurança da Informação da **PATRUS** deve ser observada, obrigatoriamente,por todos os Usuários dos Recursos de TI.

Art. 7º Os Recursos de TI, bem como toda informação da **PATRUS** ou gerada, adquirida, armazenada, processada ou transmitida pela mesma, são de titularidade da **PATRUS**.

Deveres Gerais dos Usuários

Art. 8º Os Usuários devem utilizar os Recursos de TI para fins estritamente profissionais, sempre em conformidade com a Política de Segurança da Informação da **PATRUS**, os ditames morais e os preceitos legais.

Art. 9º Os Usuários devem tomar todos os devidos cuidados para que as informações que circulam ou que estiverem armazenadas no âmbito dos Recursos de TI somente possam ser acessadas por quem tenha autorização para fazê-lo.

Art. 10. Os Usuários não podem, em nenhuma hipótese, utilizar os Recursos de TI para acesso, visualização, divulgação, transmissão ou armazenamento de qualquer tipo de conteúdo ou informação que possa se enquadrar nos seguintes casos:

I – conteúdo que possa ser considerado inadequado, imoral ou ilegal;

II – conteúdo que contenha ou faça referência a qualquer forma de discriminação: racismo, pedofilia, pornografia, prática de crimes, incitação à violência, ou informações falsas, caluniosas, injuriosas ou difamatórias;

III – conteúdo que viole a propriedade intelectual de terceiros, notadamente direitos de patentes ou marcas, segredos industriais, regras de licenciamento de *softwares* ou direitos autorais, ou ainda que configurem concorrência desleal ou outros crimes tipificados na Lei de Propriedade Industrial (Lei n. 9.279/96) e na Lei de Direito Autoral (Lei n. 9.610/98);

IV – conteúdo que caracterize a produção, oferta, distribuição, venda ou difusão de códigos ou programas de computador cujo objetivo seja invadir dispositivo informático 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 titular do dispositivo, ou instalar vulnerabilidades para obter vantagem ilícita;

V – conteúdo que caracterize produção, oferta, distribuição, venda ou difusão de códigos ou programas de computador cujo objetivo seja interromper serviço telemático ou de informação de utilidade pública, ou impedir e dificultar seu restabelecimento (vírus, *worms*[1], cavalos de tróia, *malware*[2], etc.);

VI – qualquer outro tipo de conteúdo de caráter malicioso que possa ser caracterizado como vírus, *worms*, cavalos de tróia ou programa que permita o controle de outros computadores;

VII – conteúdo que caracterize *spam* de propagandas de quaisquer produtos ou assemelhados;

VIII – conteúdo que desmereça as opiniões e os posicionamentos oficiais adotados pela **PATRUS**.

§ 1º Caso o Usuário se depare com quaisquer dos conteúdos mencionados neste artigo deve, imediatamente, notificar a **PATRUS** por meio de seu Canal de Denúncias.

Art. 11. O Usuário não pode, em hipótese alguma, adotar condutas cujo objetivo seja burlar os mecanismos de segurança adotados no âmbito dos Recursos de TI

[1] *Worm* é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar.
[2] *Malware* é um programa de computador destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não).

Art. 12. Os Usuários devem observar todas as normas de conduta previstas na Política de Segurança da Informação da **PATRUS**.

Monitoramento e Controle

Art. 13. A **PATRUS** reserva para si o direito de monitorar e de interferir no uso dos Recursos de TI, sempre que julgar necessário, com o propósito de verificar o cumprimento dos padrões de segurança estabelecidos pela sua Política de Segurança da Informação

Art. 14. Sempre que possível, a **PATRUS** armazenará os dados e os registros relativos a todas as atividades realizadas em cada Conta de Usuário, através dos de TI.

§1º As trilhas de auditoria implementadas nas aplicações desenvolvidas ou utilizadas no âmbito da **PATRUS** devem conter, sempre que possível, os seguintes dados:

I – sistema ou aplicação utilizada pelo Usuário;

II – dados da Conta de Usuário utilizada para acesso;

III – data e hora de acesso ao sistema ou aplicação;

IV – especificação da operação realizada pelo usuário.

§ 2º As trilhas de auditoria permitem a completa rastreabilidade do processo de tratamento de dados na infraestrutura de Tecnologia da Informação da **PATRUS** feito por qualquer um de seus operadores.

CAPÍTULO 2 – IDENTIDADE DE USUÁRIOS E SENHAS

Disposições Gerais

Art. 15. O Setor de TI atribui a cada um dos Usuários uma Conta de Usuário, a qual deve ser utilizada exclusivamente para fins profissionais.

§ 1º A cada Usuário, devidamente identificado e individualizado, somente pode ser atribuída uma única Conta de Usuário para acesso aos Sistemas Corporativos.

§ 2º Em caráter excepcional, o Setor de TI pode criar Contas de Usuário genéricas, isto é, que podem ser acessadas por mais de um Usuário, sendo que cada uma dessas contas ficará sob a responsabilidade do Gestor da área que a utilizar.

Art. 16. O Usuário é responsável pela movimentação e utilização das Contas de Usuários que lhe forem atribuídas, cabendo-lhe

sempre observar as normas integrantes da Política de Segurança da Informação da PATRUS e demais normas da Instituição.

Art. 17. Todos os Usuários somente podem ter acesso aos Sistemas Corporativos por meio de suas respectivas Contas de Usuário.

Parágrafo único. O Usuário somente pode acessar as informações e os arquivos cujo acesso lhe for permitido.

Senhas

Art. 18. A senha de acesso vinculada à Conta de Usuário tem caráter pessoal e intransferível, sendo vedado ao Usuário revelá-la a quem quer que seja, bem como solicitar a senha de outros usuários.

§ 1º Os Usuários devem criar senhas que:

I – sejam fáceis de lembrar e difíceis de serem descobertas por terceiros;

II – não contenham caracteres idênticos consecutivos ou grupo de caracteres somente numéricos ou alfabéticos;

III – não sejam baseadas em dados de fácil adivinhação ou na obtenção de informações pessoais, tais como nome,

sobrenome, datas importantes, placas de carros, números de documentos, dentre outras.

§ 2º São exemplos de senhas seguras aquelas que não contêm mais de 2 (dois) caracteres consecutivos do nome completo do titular da Conta de Usuário e que contêm caracteres das quatro categorias seguintes:

I – caracteres maiúsculos (de "A" a "Z");
II – caracteres minúsculos (de "a" a "z");
III – base 10 dígitos (0 a 9);
IV – caracteres não alfabéticos (ex: !, $, #, %).

§ 3º As senhas criadas para acesso aos Sistemas Corporativos devem ser utilizadas exclusivamente para este fim, e nunca em sistemas de outras empresas ou serviços, como e-mails pessoais, redes sociais, Internet Banking, dentre outros.

§ 4º O Usuário deve ficar atento aos locais de guarda das senhas criadas para acesso aos Sistemas Corporativos, evitando anotá-las e deixá-las expostas a terceiros, assumindo a responsabilidade sobre as mesmas.

Art. 19. As regras acima apresentadas para a criação de senhas seguras devem ser também adotadas, sempre que possível,

quando da criação e alteração de senhas nos sistemas adotados pela **PATRUS**.

Art. 20. Caso haja necessidade de redefinir a senha vinculada à Conta de Usuário, o Usuário deve solicitá-la ao Setor de Tecnologia da Informação.

Bloqueio e Desativação de Contas de Usuário

Art. 21. As Contas de Usuários relativas a Usuários que não mantiverem mais vínculo com a **PATRUS** serão desativadas na data do término do vínculo, cabendo à liderança do setor em que ocorreu o desligamento notificar o fato ao setor de Recursos Humanos e de TI.

§ 1º Em caso de desligamento da liderança do setor, cabe ao diretor responsável pela área notificá-lo ao setor de Recursos Humanos e de TI.

§ 2º Os dados e informações referentes à Conta de Usuário desativada devem ser preservados por um prazo de trinta dias após o término do vínculo do usuário com a **PATRUS**

§ 3º Ainda que, por algum motivo, a Conta de Usuário não tenha sido desativada na data do término do vínculo entre o Usuário e a **PATRUS**, o Usuário não pode utilizá-la para acessar os Sistemas Corporativos.

§ 4º Em caso de bloqueios emergenciais, o Setor de RH deve entrar em contato com o Setor de TI solicitando o bloqueio.

CAPÍTULO 3 – CANAIS OFICIAIS DE COMUNICAÇÃO

Disposições Gerais

Art. 22. Constituem canais oficiais de comunicação da **PATRUS** todas as funcionalidades disponibilizadas pelo Google Workspace, como o e-mail corporativo e a plataforma Hangouts.

Art. 23. Os Usuários devem fazer uso dos canais oficiais de comunicação sempre que for necessária a transmissão de quaisquer informações relativas às atividades da **PATRUS**, sendo expressamente vedado o envio por canais alternativos de:

I – dados pessoais;

II – informações estratégicas da **PATRUS**, mas não limitadas a informações financeiras, contratuais com terceiros e planos de ação.

Art. 24. O Usuário assume a responsabilidade pelas informações por ele compartilhadas ou trafegadas por meio de canais não oficiais de comunicação – por exemplo, e-mail particular e aplicativos de mensagens instantâneas (como o *WhatsApp* ou o *Telegram*).

Uso de Correio Eletrônico Corporativo (*E-mail* Corporativo)

Art. 25. É dever do Usuário fazer uso adequado da conta de e-mail corporativo que lhe for atribuída, sendo vedados:

I – o envio de mensagens com informações particulares, ou seja, que dizem respeito à esfera íntima do Usuário;

II – o envio de mensagens com informações confidenciais, sem a devida autorização formal de seu Gestor ou pessoa responsável por aquela informação;

III – o envio de mensagens que contenham arquivos anexados cujo conteúdo não possua relação com as atividades desempenhadas pela **PATRUS**; que veiculam propagandas,

boatos, ou que se enquadrem nas hipóteses previstas no art. 9º desta Política;

IV – o cadastramento da conta de e-mail corporativo em sites com finalidades particulares (como sites de mídias sociais ou de compra e venda online);

V – o envio de mensagens com cópia aberta para mais de oito pessoas, devendo-se fazer uso, quando necessário, da cópia oculta;

VI – a utilização do correio eletrônico corporativo durante o período de férias e de afastamento por licença.

VII – Qualquer forma de compartilhamento de e-mails que venham identificados com a proibição de envio a terceiros, como aqueles oriundos do sistema do Canal de Denúncias.

Art. 26. Cabe ao usuário realizar verificações frequentes em sua conta de e-mail, eliminando arquivos e mensagens desnecessárias à execução das atividades da **PATRUS**

Art. 27. O Usuário é responsável pelas mensagens transitadas em sua conta de e-mail corporativo e, no caso de contas genéricas, do Gestor da área.

CAPÍTULO 4 – Uso da Internet

Disposições Gerais

Art. 28. O serviço de Internet é disponibilizado pela **PATRUS** exclusivamente para atividades relacionadas aos seus negócios e serviços, para a comunicação com clientes e fornecedores e para pesquisas de tópicos pertinentes e obtenção de informações empresariais úteis, no sentido de manter os níveis mais altos de produtividade, qualidade e atualização tecnológica e de promover o desenvolvimento profissional de seu pessoal.

Parágrafo único. A disponibilização do serviço de Internet pela **PATRUS** pode ser condicionado ao aceite, pelo Usuário, dos termos de uso, variantes conforme o público.

Art. 29. Sempre que possível, o acesso à rede de Internet, por qualquer meio, somente deve ser possibilitado ao Usuário devidamente autenticado em sua Conta de Usuário.

Art. 30. A **PATRUS** pode restringir ou bloquear o acesso a determinados sites ou categorias de sites por meio da adoção de filtros de conteúdo.

Parágrafo único. Pode ser restringido ou bloqueado o acesso a sites que:

I – veiculem qualquer tipo de conteúdo ilícito ou imoral;

II – apresentem risco de comprometimento da produtividade, tais como sites que demandam alto consumo de banda (*streaming*, vídeo, *peer-to-peer* e outros);

III – apresentem risco à segurança das informações ou dados da **PATRUS**, possuindo alto índice de disseminação de pragas virtuais;

IV – permitam a realização de publicações em blogs e mídias sociais pelos Usuários.

Art. 31. A **PATRUS** reserva para si o direito de monitorar o uso de qualquer dado ou informação que trafegue na infraestrutura de Tecnologia da Informação.

Art. 32. O Usuário tem ciência de que qualquer dado ou informação tratado(a) na infraestrutura de Tecnologia da Informação da **PATRUS** não é de sua exclusiva privacidade.

Uso de Redes Sem Fio

Art. 33. O acesso via tecnologia de acesso à rede sem fio das unidades da **PATRUS** por equipamentos móveis é um serviço de comunicação disponibilizado pelo **PATRUS** exclusivamente para atividades relacionadas aos seus negócios e serviços, e deve ser

utilizado para fins corporativos apenas durante o expediente de trabalho.

Art. 34. A **PATRUS** reserva para si o direito de cancelar ou restringir o acesso de qualquer usuário à rede sem fio por decisão administrativa, razões técnicas ou violações das regras definidas na Política de Segurança da Informação da **PATRUS**.

Art. 35. Qualquer acesso via tecnologia sem fio à rede de Internet da **PATRUS** pode ser rastreado.

Art. 36. Somente os dispositivos de propriedade da **PATRUS** e os disponibilizados por terceiros, nos casos previstos em contrato, que estiverem em conformidade com o padrão estipulado pelo Setor de TI devem ser utilizados para acesso à rede de Internet da **PATRUS**.

Deveres dos Usuários

Art. 37. O Usuário deve conduzir adequadamente o uso da Internet, sempre em conformidade com a lei e com a Política de Segurança da Informação da **PATRUS**.

Art. 38. Os Usuários, ao utilizarem a rede de Internet da **PATRUS** não podem:

I – acessar, visualizar, armazenar, divulgar ou repassar qualquer site, portal, página da Internet ou material com conteúdo inadequado ou ilegal, tais como aqueles que contenham ou façam referência a qualquer forma de discriminação, ao racismo, à pedofilia, à pornografia, à prática de crimes, à incitação à violência, a fatos que não sejam verdadeiros, a fatos ou informações caluniosas, a fatos ou informações injuriosas, a fatos ou informações difamatórias, a fatos ou informações que contrariem a moral e os bons costumes, a fatos ou informações que violem direitos autorais, regras de licenciamento de *softwares* e direitos relativos à propriedade, à privacidade e à proteção da propriedade industrial;

II – acessar, visualizar, armazenar, divulgar ou repassar qualquer site, portal, página da Internet ou material, tais como salas de bate-papo (*chat*), *blogs*, aplicativos de mensagens instantâneas e redes sociais, para acessar conteúdo alheio às atividades profissionais da **PATRUS**, como arquivos de som e vídeo que não tenham relação com o ambiente corporativo;

III – armazenar ou trocar dados de conteúdos autorais não autorizados nos termos da Lei n. 9.610/98 e normas correlatas;

IV – fazer *download* ou distribuição de quaisquer *softwares* sem autorização prévia e formal do Setor de TI;

V – efetuar *upload* de qualquer *software* licenciado da **PATRUS** sem a expressa autorização do Setor de TI;

VI – acessar e propagar, deliberadamente, qualquer tipo de conteúdo malicioso, como vírus, *worms*, cavalos de tróia ou programas que permitam o controle de outros computadores, bem como *spam* de propagandas de quaisquer produtos ou assemelhados;

VII – utilizar ferramentas e serviços de troca de mensagens não autorizados pelo Setor de TI;

VIII – utilizar qualquer ferramenta com o intuito de burlar a segurança dos Recursos de TI da **PATRUS**, visando ao acesso a sites bloqueados ou o acesso não autorizado à Internet;

IX – Publicar, em nome da **PATRUS**, comentários em mídias sociais, sites, blogs ou qualquer outra rede de relacionamento ou colaboração;

X – publicar comentários em mídias sociais, sites, blogs ou qualquer outra rede de relacionamento ou colaboração que relacione a **PATRUS** a assuntos não condizentes com suas atividades.

Art. 39. O acesso à rede de Internet da **PATRUS** deve ser efetuado somente por meio de equipamentos autorizados pelo **PATRUS**, registrados, identificados e homologados pelo Setor de TI, que devem seguir, obrigatoriamente, os padrões de segurança adotados pela **PATRUS**.

CAPÍTULO V – USO E ADMINISTRAÇÃO DA REDE CORPORATIVA

Art. 40. A Rede Corporativa somente deve ser utilizada pelos Usuários que tiverem permissão para acessá-la, que estiverem devidamente autenticados em suas respectivas Contas de Usuário, utilizando aparelhos também autorizados e para fins estritamente profissionais.

Parágrafo único. O Usuário somente pode acessar as informações e os arquivos cujo acesso lhe for permitido pelo próprio sistema, por orientações de seu Gestor ou por força das disposições do contrato que o vincula à **PATRUS**.

Art. 41. O Usuário deve usar adequadamente a Rede Corporativa, utilizando-a exclusivamente para a consulta de dados e informações relacionados às atividades da **PATRUS** sendo vedada sua utilização para o armazenamento de qualquer conteúdo ilícito, imoral ou que possa ser enquadrado nas disposições do art. 9º deste documento.

Art. 42. Qualquer acesso à Rede Corporativa e qualquer atividade nela realizada pelo Usuário podem ser rastreados pela **PATRUS**..

Art. 43. O acesso remoto à Rede Corporativa somente pode ocorrer mediante VPN, cuja liberação é realizada pelo Setor de TI com a assinatura de termo de responsabilidade pelo Usuário.

CAPÍTULO 6 – USO E MANUSEIO DE ESTAÇÕES DE TRABALHO, EQUIPAMENTOS E PROGRAMAS DE COMPUTADOR DA PATRUS

Disposições Gerais

Art. 44. As normas previstas nesta seção regulam a utilização de todos os equipamentos de informática e *softwares* integrantes dos Recursos de TI não tratados especificamente em outras seções deste documento.

Art. 45. A utilização de estações de trabalho ou de equipamentos da **PATRUS**, conectados ou não à rede de Internet ou à rede de dados da **PATRUS**, por qualquer meio, somente deve ser possibilitada ao Usuário devidamente autenticado em sua Conta de Usuário.

Art. 46. Os usuários devem fazer uso adequado dos equipamentos de informática (*hardware*) e programas de computador (*software*) da **PATRUS** conforme as seguintes orientações:

I – para conectar qualquer equipamento de informática (computadores, *notebooks*, *switches*, *hubs*, etc.) na rede de dados ou na rede de Internet da **PATRUS**, o Usuário deve consultar previamente o Setor de TI, via ordem de serviço, que autorizará ou não a solicitação, a seu exclusivo critério;

II – o Usuário não pode alterar as configurações-padrão de *hardware* e *software* dos equipamentos;

III – o Usuário não pode violar os lacres dos computadores e demais equipamentos eletrônicos da **PATRUS**, a fim de não comprometer a segurança e a garantia desses recursos;

IV – o Usuário não pode compartilhar pastas ou arquivos dos computadores e demais equipamentos eletrônicos que permitem o armazenamento de informações sem a utilização de senhas de proteção e a definição dos demais Usuários autorizados a acessá-los;

V – O Usuário não pode utilizar nem instalar *softwares* não autorizados ou sem licença de uso nas estações de trabalho ou nos equipamentos eletrônicos da **PATRUS**, tais como:

a) jogos ou *softwares* de entretenimento;

b) *softwares* gratuitos, temporários ou compartilhados (*freewares* e sharewares) que não se relacionem às atividades da **PATRUS** e que não sejam autorizados pelo Setor de TI;

c) *softwares* desenvolvidos particularmente por um Usuário e não autorizados pelo Setor de TI;

d) *softwares* distribuídos por meio de revistas ou obtidos (*download*) via Internet;

e) cópias sem licença de *softwares* autorizados;

VI – ficam vedados o acesso, o armazenamento ou a troca de dados, por qualquer modalidade, de conteúdo que possa ser enquadrado nas hipóteses do art. 9º deste documento;

VII – Os Usuários não podem utilizar os equipamentos de informática da **PATRUS** para fazer envio e/ou armazenamento de arquivos de músicas, filmes e outros tipos de documentos não relacionados com as atividades da **PATRUS**, salvo mediante expressa autorização;

VIII – os equipamentos de informática da **PATRUS** não devem ser utilizados para efetuar envio (*upload*) de dados e documentos da **PATRUS** que sejam confidenciais ou reservados, sem a autorização prévia e formal do Gestor ou da pessoa responsável.

Art. 47. O Usuário deve realizar o encerramento da sessão sempre que houver necessidade de se ausentar de sua estação de trabalho, de forma a evitar acessos indevidos.

Art. 48. O Usuário deve tomar todos os cuidados necessários para a preservação dos Recursos de TI que lhe foram confiados,

sempre em observância às normas de guarda de patrimônio da **PATRUS**.

Uso dos Computadores Móveis Disponibilizados pela PATRUS

Art. 49. Somente computadores móveis de propriedade da **PATRUS** e os utilizados por terceiros, nos casos previstos em contrato, que estiverem em conformidade com o padrão estipulado pelo Setor de TI, devem ser utilizados para acesso à rede de dados ou à rede de Internet da **PATRUS**.

Art. 50. Os computadores móveis devem acessar somente a rede de dados ou a rede de Internet após as devidas validações realizadas pelo Setor de TI

Art. 51. Os computadores móveis são disponibilizados aos Usuários como ferramenta de apoio às atividades profissionais e seu uso deve ser restrito às atividades realizadas no âmbito da **PATRUS**.

Art. 52. O uso dos computadores móveis somente é permitido a Usuários autorizados e autenticados em suas respectivas Contas

de Usuário, e sua retirada de qualquer uma das unidades da **PATRUS** deve ser autorizada pelo Setor de TI.

Art. 53. O usuário que utiliza computadores móveis disponibilizados pela **PATRUS** deve observar as instruções dos fabricantes para sua proteção e seu manuseio, além das diretrizes da **PATRUS** previstas nesta Política de Segurança da Informação.

Art. 54. Somente podem ser instalados nos computadores móveis, *softwares*, aplicações e *plugins* que atendam às seguintes regras:

I – nos *notebooks*, *netbooks* e *laptops*, somente os *softwares* homologados pelo Setor de TI;

II – nos *tablets*, *palmtops* e *smartphones*, *softwares* do fabricante necessários para o funcionamento do equipamento e seus periféricos e *softwares* homologados pelo Setor de TI.

Art. 55. Em viagem ou fora do espaço físico da **PATRUS**, o Usuário deve tomar todos os cuidados para proteger o computador móvel e os dados nele contidos, como não deixá-lo sozinho ou permitir a visualização do seu conteúdo por terceiros.

Art. 56. As informações da **PATRUS** armazenadas nos computadores móveis devem ser protegidas pelo Usuário contra vazamento e alterações não autorizadas.

Art. 57. O Setor de TI deve efetuar a configuração do antivírus, quando disponível para o computador móvel, celulares corporativos, ou qualquer outro dispositivo informático, de modo a realizar a atualização automática via Internet, quando o Usuário estiver fora do local onde exerce suas atividades profissionais

Art. 58. O uso externo em computador móvel de qualquer mídia removível, tais como cartões de memória, CDs, DVDs, *pen drives* e HD externo, dentre outros, deve ter sua utilização limitada a:

I – cópia de segurança (*backup*) de trabalho.
II – Transferência de dados vindos de fonte externa confiável.

Art. 59. É vedado ao Usuário alterar as configurações de rede sem fio.

Art. 60. Quando da devolução do computador móvel, o Usuário deve entregar todos os acessórios recebidos (fonte de alimentação externa, mouse sem fio, HD externo, etc.).

Art. 61. Quando não estiver em uso, o computador móvel deve ficar armazenado em local seguro.

Parágrafo único. No caso do *notebook*, o Usuário deve realizar *logout* com *Ctrl* + *Alt* + *Delete* quando ele não estiver em uso, e o *tablet* deve ser protegido obrigatoriamente com senha de acesso.

Manutenção e Movimentação de Equipamentos

Art. 62. Os serviços de manutenção de equipamentos e acessórios da **PATRUS**, bem como de *softwares*, devem ser executados somente pelo Setor de TI e fornecedores autorizados.

Art. 63. Similarmente, os serviços de movimentação de equipamentos e acessórios da **PATRUS** devem ser executados somente pelo Setor de TI e fornecedores autorizados.

Parágrafo único. Caso, durante a manutenção, seja identificada a existência de *softwares* não autorizados, o Setor de TI deve comunicar, via ordem de serviço, o fato ao Gestor ao qual o Usuário se vincula, que tomará as medidas cabíveis, conforme disposto neste documento.

Art. 64. O Usuário deve acompanhar a realização da manutenção preventiva ou corretiva de uma estação de trabalho sob sua responsabilidade, quando esta for realizada no seu ambiente de trabalho.

Art. 65. Antes do descarte de estações de trabalho, de computadores móveis danificados que demandarem substituição definitiva, ou de equipamentos alugados serem devolvidos, o Setor de TI deve providenciar a exclusão definitiva das informações neles contidas, tornando impossível sua recuperação.

Proibições

Art. 66. Ficam vedadas aos Usuários que utilizem computadores móveis da **PATRUS** as seguintes condutas:

I – emprestar os computadores móveis sem autorização da pessoa competente;

II – deixar o computador móvel desprotegido em local público, no local de trabalho ou em locais de alto risco de furto ou roubo, tais como carros ou outros meios de transporte, quartos de hotéis, centros de convenção, salas de reunião, rodoviárias, aeroportos, etc;

III – conectar qualquer recurso ou mídia removível não autorizada pelo Setor de TI nas estações de trabalho e computadores móveis;

IV – conectar qualquer estação de trabalho na rede de Internet ou na rede de dados da **PATRUS** sem autorização do Setor de TI;

V – compartilhar diretórios (pastas) das estações de trabalho com terceiros;

VI – violar os lacres dos equipamentos que integram os Recursos de TI da **PATRUS**;

VII – Acessar, armazenar ou trocar dados que possam se enquadrar nas definições do art. 9º deste documento;

VIII – alterar a configuração-padrão de *hardware* ou *software* dos equipamentos que estiverem sob seu controle;

IX - salvar arquivos na área de trabalho dos computadores móveis ou na pasta C: deve-se salvar tais arquivos nas pastas (locais ou em nuvem) designadas pelo setor responsável ou pelo departamento de TI.

X – baixar arquivos não relacionados às atividades desenvolvidas pela **PATRUS**.

CAPÍTULO 7 – USO DE MÍDIAS SOCIAIS

Disposições Gerais

Art. 67. O Setor de Comunicação e Marketing é responsável pela administração dos perfis oficiais da **PATRUS** nas Mídias Sociais, reservando-se o direito de avaliar e responder a qualquer comentário publicado nestes perfis.

Art. 68. Se, a qualquer tempo, algum Usuário publicar ou postar conteúdo que envolva o nome ou a imagem da **PATRUS** deve, primeiramente, deixar claro que o conteúdo publicado contém apenas sua opinião pessoal, desvinculada da opinião da **PATRUS** e que assume toda a responsabilidade perante a publicação.

Art. 69. Recomenda-se que, na situação descrita no artigo anterior, o Usuário inclua em sua postagem ou publicação a seguinte nota: "As ideias contidas nesta publicação são de cunho pessoal e não refletem a opinião da **PATRUS**".

Art. 70. Os Usuários não devem fazer uso das mídias sociais de maneira que comprometa a confidencialidade de dados, imagens, informações sigilosas, segredos comerciais, reputacionais ou de quaisquer ativos de titularidade da **PATRUS**, sob pena de tal conduta ser considerada prática de concorrência

desleal, nos termos do art. 195 da Lei de Propriedade Industrial (Lei n. 9.279/96, de constituir crime de calúnia, difamação ou injúria, conforme os arts. 138, 139 e 140 do Código Penal, ou de ensejar responsabilização civil, conforme os arts. 186, 187 e 927 do Código Civil.

Art. 71. Fica proibida a publicação, a qualquer tempo, de toda comunicação envolvendo assuntos internos à **PATRUS**, tais como informações estratégicas, financeiras, técnicas, administrativas, sem prejuízo de outras, nas Mídias Sociais e outras formas de divulgação pública na Internet.

Art. 72. É vedado ao Usuário divulgar informações acerca do trabalho desenvolvido no âmbito da **PATRUS** ou do seu ambiente de trabalho, além de projetos, resultados e outras informações a que tenha acesso em razão do cargo ou função desempenhada.

Art. 73. Caso o Usuário tenha interesse em divulgar informações que sejam de potencial interesse do público-alvo da **PATRUS**, inclusive seus clientes, deve solicitar análise do Setor de Comunicação e Marketing, indicando o conteúdo que deseja ver publicado nos canais oficiais.

Art. 74. Somente é permitida a publicação de imagens ou informações de Colaboradores da **PATRUS** caso haja a autorização prévia e por escrito do colaborador para tanto.

Parágrafo único. Cabe aos Gestores de cada setor gerenciar a coleta e a assinatura dos termos de cessão de imagem, a serem disponibilizados pelo Setor de Comunicação e Marketing.

Art. 75. É vedado o uso do endereço de e-mail corporativo da **PATRUS** para fins de cadastramento em Mídias Sociais, *websites*, fóruns de discussão, sites de *e-commerce* e serviços de computação em nuvem, salvo quando utilizados pela **PATRUS**.

Monitoramento de Conteúdos Publicados nas Mídias Sociais

Art. 76. A **PATRUS** monitora, em tempo real, todos os conteúdos e comentários publicados e compartilhados nas Mídias Sociais que envolvam o nome ou a marca da **PATRUS** ou de seus gestores.

Art. 77. O resultado do monitoramento permite a **PATRUS** impor sanções, tomando as medidas cabíveis quando necessário, conforme a Política de Segurança da Informação e demais normas internas existentes.

Art. 78. Não serão toleradas publicações que veiculam o nome da **PATRUS** a qualquer tipo de conteúdo mencionado no art. 9º desta Política de Segurança da Informação; que veiculem dados

pessoais, sobretudo de colaboradores, sem a autorização prévia e formal do titular; ou que digam respeito a informações estratégicas da **PATRUS**..

Art. 79. No que diz respeito a postagens realizadas por Colaboradores, Bolsistas, membros da Diretoria, Fornecedores e Prestadores de Serviços, em quaisquer Canais de Comunicação, cabe a estes, exclusivamente, a responsabilidade pelo conteúdo da publicação e divulgação.

Art. 80. Igualmente, quaisquer postagens realizadas pelas filiais, em quaisquer Canais de Comunicação, são de responsabilidade exclusiva da própria filial que publicou o conteúdo.

CAPÍTULO 8 – ACESSO REMOTO EXTERNO

Disposições Gerais

Art. 81. As normas deste capítulo são aplicáveis aos Usuários que acessem remotamente os Recursos de TI da **PATRUS**.

Parágrafo único. O acesso remoto somente poderá ser concedido aos Usuários nos casos em que o exercício pleno de

suas funções assim o exigirem, mediante assinatura de termo de acesso.

Art. 82. A **PATRUS** disponibilizará o acesso remoto ao Usuário com o único intuito de facilitar sua atuação quando em trânsito, em casos de força maior ou quando for inviável o acesso presencial à rede local nas dependências da **PATRUS** fora do horário de expediente, em detrimento da necessidade de eventual deslocamento.

Art. 83. A **PATRUS** reserva para si o direito de monitorar e interferir no acesso remoto, com a finalidade de verificar e de garantir o cumprimento dos padrões mínimos de segurança estabelecidos nesta Política de Segurança da Informação.

Art. 84. O equipamento utilizado para o acesso remoto deve atender, ainda, aos seguintes requisitos mínimos de segurança:

I – ter instalado sistema operacional licenciado e atualizado;
II – ter instalado programa antivírus licenciado e atualizado.

Art. 85. A **PATRUS** reserva para si o direito de incluir regras sistêmicas que impeçam o acesso por meio de equipamento em desacordo ao disposto nos artigos anteriores, quando julgar que

a falta desses requisitos esteja colocando em risco seu ambiente operacional.

Art. 86. O acesso remoto somente é permitido se realizado em conformidade com as orientações do Setor de TI, que objetivam garantir maior integridade no processo de autenticação do usuário e proteção ao sistema contra acessos não autorizados.

Art. 87. Durante a sessão de acesso remoto, o Usuário deve executar apenas atividades condizentes com suas respectivas funções, não utilizando os Recursos de TI para fins pessoais.

Art. 88. O direito ao acesso remoto será revogado permanentemente ou temporariamente nas seguintes situações:

I – desligamento do Empregado ou Colaborador;
II – detecção da não necessidade do acesso remoto;
III – não observância das regras de acesso remoto.

CAPÍTULO 9 – PROTEÇÃO FÍSICA DOS ATIVOS DE INFORMAÇÃO

Disposições Gerais

Art. 89. As normas previstas neste capítulo regulamentam o uso e a proteção dos Recursos de TI, visando resguardar os equipamentos de acesso físico não autorizado, da ação de vírus, de erros, de omissões e de uso indevido, bem como promover o descarte seguro de dados.

Art. 90. Os Recursos de TI são de propriedade da **PATRUS**, não podendo ser extraviados, copiados, pirateados ou armazenados em dispositivos que não sejam de propriedade e utilização da **PATRUS**.

Art. 91. O uso e o acesso a sistemas críticos devem ser monitorados com o objetivo de detectar atividades não autorizadas.

Descarte Seguro de Mídias de Armazenamento

Art. 92. As Mídias de Armazenamento devem ser descartadas nos seguintes casos:

I – mídias que passaram do prazo de validade ou se tornaram inutilizáveis por alguma outra razão;

II – devoluções de dispositivos defeituosos que estiverem no prazo de garantia;

III – discos ópticos com informações que deixaram de ser necessárias;

IV – papéis com dados obsoletos para a **PATRUS** que já não precisam estar impressos ou que são redundantes (ou seja, que estão presentes em outras Mídias de Armazenamento).

Art. 93. Os papéis que contiverem dados pessoais ou quaisquer outras informações estratégicas da **PATRUS** devem ser fragmentados antes de serem descartados e não podem ser utilizados como rascunho

Segurança Física das Portarias

Art. 94. A concessão de acesso aos prédios das unidades da **PATRUS** está sujeita a controle.

§ 1º O acesso de Empregados, Colaboradores, membros da da Diretoria, Estagiários e Bolsistas será permitido mediante identificação biométrica e utilização de crachás.

§ 2º O acesso de Prestadores de Serviços, Fornecedores e Visitantes será permitido somente após cadastro nas portarias, sendo necessário o fornecimento de documento pessoal e de informações sobre o motivo da visita e o local de destino.

Segurança Física do *Data Center*

Art. 95. As salas que contêm os servidores da **PATRUS** são áreas de acesso restrito a Empregados, Colaboradores, Prestadores de Serviços ou Fornecedores autorizados, que devem se sujeitar às normas de utilização do ambiente.

Art. 96. Cabe ao (coordenador, gerente ou superintendente) de Tecnologia da Informação definir os acessos permitidos às salas de servidores da **PATRUS**, bem como revisar esses acessos mensalmente.

Art. 97. Não é permitido o acesso às salas de servidores à pessoa que portar objetos pessoais, como bolsas, mochilas, sacolas, cadernos, alimentos ou ferramentas, salvo necessidade e com o devido acompanhamento.

Art. 98. Não é permitido o acesso às salas de servidores à pessoa que portar qualquer tipo de dispositivo eletrônico de

processamento e armazenamento de informações, tais como *pen drives*, CDs ou DVDs, salvo necessidade e com o devido acompanhamento.

Parágrafo único. A entrada de equipamentos e ferramentas somente será permitida se comprovada sua necessidade para execução de alguma atividade.

Art. 99. É proibido fazer uso indevido de qualquer ferramenta dentro das salas que contenham os servidores da **PATRUS** que possam causar prejuízo ao ambiente, à instalação ou a qualquer equipamento da empresa.

Art. 100. É proibido filmar ou fotografar nas dependências das salas que contêm os servidores da **PATRUS**, salvo autorização prévia e por escrito do Setor de TI.

Art. 101. O acesso às salas que contenham os servidores da **PATRUS** somente será liberado às pessoas devidamente identificadas por crachá em local visível, além do uso correto da senha das portas que lhe fazem a segurança.

Parágrafo único. É proibido o fornecimento de senhas a pessoas não autorizadas para acesso às salas que contêm servidores.

Antivírus

Art. 102. O Setor de TI é responsável por instalar antivírus nos equipamentos móveis e estações de trabalho da **PATRUS** com configuração que permita sua atualização recorrentemente.

Art. 103. O Setor de TI é o responsável por manter o antivírus e as correções de segurança do sistema operacional das estações de trabalho e equipamentos móveis atualizados.

Art. 104. O Setor de TI é responsável por monitorar a existência de *softwares* não autorizados nas estações de trabalho e equipamentos móveis da **PATRUS**, removendo-os, se identificados.

CAPÍTULO 10 – NORMA DE PROTEÇÃO DOS ATIVOS INTANGÍVEIS

Disposições Gerais

Art. 105. As normas constantes desta seção disciplinam o regime aplicável à propriedade dos Ativos Intangíveis criados pela **PATRUS** ou pelos Empregados, Colaboradores, Estagiários,

Bolsistas, Fornecedores ou Prestadores de Serviços enquanto vigentes seus vínculos contratuais com a empresa.

Art. 106. Os Ativos Intangíveis resultantes de trabalhos realizados em favor da **PATRUS**, regulados por acordo ou contrato firmado com Empregados, Colaboradores, Estagiários, Bolsistas, Fornecedores ou Prestadores de Serviços, serão de titularidade da **PATRUS**, exceto se disposto em contrário nos exatos termos do contrato celebrado entre as partes.

Art. 107. Ressalvado ajuste em contrário, os Ativos Intangíveis desenvolvidos por Empregados, Colaboradores, Estagiários, Bolsistas, Fornecedores ou Prestadores de Serviços da **PATRUS**, de forma colaborativa ou individual, no decorrer do contrato de trabalho ou vínculo contratual aplicável, e com a utilização de recursos, informações, segredos industriais e de negócios, materiais, instalações ou equipamentos, são de titularidade e propriedade exclusiva da **PATRUS**.

Medidas Protetivas dos Ativos Intangíveis

Art. 108. Estão vedadas as seguintes condutas consideradas potenciais riscos à segurança quanto ao uso de ativos intangíveis da **PATRUS**:

I – obter e compartilhar, sem a devida autorização ou necessidade, por meio de canais não oficiais de comunicação, dados pessoais dos Colaboradores, Empregados, Fornecedores, Estagiários, Bolsistas ou Prestadores de Serviços da **PATRUS**, caso não sejam expressamente considerados de acesso público;

II – publicar ou divulgar a terceiros informações ainda não confirmadas oficialmente pela **PATRUS** sobre suas atividades, ou as de Colaboradores, Empregados, Fornecedores, Estagiários, Bolsistas ou Prestadores de Serviços;

III – publicar, sem a devida autorização prévia e formal, imagens ou vídeos que retratam o ambiente interno da empresa.

IV – Divulgar, por qualquer motivo, informações confidenciais, tais como fórmulas, práticas, processos, designs, instrumentos, padrões ou uma compilação de informações ou dados utilizados por um negócio, projetos, segredos industriais e de negócio ou imagens do circuito interno de monitoramento;

V – utilizar de maneira não autorizada os Ativos Intangíveis da **PATRUS**, sem que antecipadamente tenha sido requisitada a devida permissão do setor competente, notadamente quanto a eventuais derivações, adaptações, reproduções ou compartilhamentos em qualquer meio;

VI – criar páginas, perfis ou qualquer outro tipo de presença online relacionados às marcas da **PATRUS**, a suas atividades ou às atividades de Colaboradores, Empregados, Fornecedores, Estagiários, Bolsistas ou Prestadores de Serviços da **PATRUS**;

VII – responder em nome da empresa qualquer discussão relacionada às atividades da **PATRUS** na Internet, sem devida autorização.

VIII – é vedada a divulgação ou compartilhamento de qualquer informação contida na íntegra da política dos contratos com prestadores de serviços, fornecedores, operadores, convênios.

Parágrafo único. Caso seja identificado qualquer incidente que possa ser enquadrado nas disposições deste artigo, recomenda-se que seja efetuada imediata comunicação do fato ao Setor de Comunicação e Marketing, que tomará as ações necessárias para prosseguir o assunto.

Medidas Protetivas dos Dados Pessoais

Art. 109. No que diz respeito ao tratamento de dados pessoais no âmbito da **PATRUS**, são proibidos:

I – o compartilhamento com pessoas não autorizadas, sobretudo que não integrem a **PATRUS**;

II – a criação de cópias ou duplicatas de documentos com dados pessoais sem que haja necessidade para tanto, ou sem a autorização do gestor ou pessoa por eles responsável;

III – a utilização para finalidade diversa daquela que justificou sua coleta;

IV – a divulgação sem autorização expressa do titular;

V – o armazenamento em mídias pessoais, como celulares e *tablets* de uso particular.

Parágrafo único. O compartilhamento de dados pessoais deve ser realizado por meio dos canais oficiais de comunicação disponibilizados pela **PATRUS**.

Art. 110. Quando do tratamento de dados pessoais, os Usuários devem sempre observar os seguintes princípios previstos na Lei 13.709/2018:

I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem a possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II – adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com

abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Art. 111. Cabe ao Usuário zelar pela segurança e pelo sigilo dos dados pessoais que lhes são confiados, podendo o mesmo ser responsabilizado por quaisquer danos que venham ser causados em caso de descumprimento das normas aqui previstas.

CAPÍTULO 11 – NORMA DE GERAÇÃO E PRESERVAÇÃO DE EVIDÊNCIAS

Disposições Gerais

Art. 112. Nesta seção, estabelecem-se procedimentos que regulamentam a notificação, o registro e o tratamento de Incidentes de Segurança da Informação e de Fragilidades em Sistemas ou Serviços identificadas pelos Usuários e que possam ter impactos na segurança dos Recursos de TI ou dos Ativos Intangíveis da **PATRUS**, visando permitir o controle e a adoção de medidas corretivas em tempo hábil.

Art. 113. Todos os Usuários devem, obrigatoriamente, notificar, conforme definido nesta seção, qualquer Incidente de Segurança da Informação ou Fragilidades em Sistemas ou Serviços da

PATRUS, imediatamente após sua identificação ou suspeita de sua identificação.

Incidentes de Segurança da Informação

Art. 114. São considerados exemplos de Incidentes de Segurança da Informação ou Fragilidades em Sistemas ou Serviços que devem ser notificados:

I – falhas de sistema de informação ou perda de serviços;

II – código malicioso;

III – negação de serviço (DDoS);

IV – erros resultantes de dados incompletos ou inconsistentes;

V – violações de confidencialidade e integridade das informações;

VI – indisponibilidade das informações;

VII – uso impróprio de sistemas de informação;

VIII – perda de serviço, equipamento ou recursos;

IX – erros humanos;

X – violações da Política de Segurança da Informação da **PATRUS**;

XI – violações de procedimentos de segurança física;

XII – mudanças não controladas ou não previstas de sistemas;

XIII – mau funcionamento de *software* ou *hardware*;

XIV – violações de acesso;

XV – tentativas de invasão física ou lógica;

XVI – tentativas de fraude;

XVII – sinistros envolvendo ativos de informação;

XVIII – vulnerabilidades em *softwares* ou aplicativos.

Art. 115. Os incidentes de Segurança da Informação devem ser comunicados ao Gestor da área de sua ocorrência e ao Setor de TI, da maneira mais rápida possível e, posteriormente, formalizados por meio do Canal de Denúncias.

§ 1º Ao reportar o incidente de Segurança da Informação, o Usuário deve relacionar todos os detalhes, tais como mensagens da tela, comportamento estranho, não conformidade ou violações da Política de Segurança da Informação da **PATRUS**.

§ 2º O Usuário não deve tomar nenhuma ação própria para solucionar o Incidente de Segurança da Informação, mas reportá-lo imediatamente, conforme disposto no *caput* deste artigo.

§ 3º Os Usuários não devem testar Fragilidades em Sistemas ou Serviços, mas reportar sua suspeita ao Setor de TI imediatamente, pois esse teste pode causar danos e ser interpretado como uso impróprio desses sistemas ou serviços.

§ 4º Dependendo do grau de confidencialidade e sigilo requerido, o Usuário que enviou a notificação via e-mail pode não ser

comunicado sobre as medidas tomadas para a solução do incidente.

Art. 116. Após a notificação, o Incidente de Segurança da Informação será categorizado (*hardware/software*), priorizado (urgência/impacto) e investigado pela Gerência do Setor de TI.

Parágrafo único. Sempre que tomar conhecimento de algum Incidente de Segurança da Informação, o setor ou a pessoa responsável pela informação ou pelo equipamento deve preservar as informações relacionadas ao incidente, bem como informar à Gerência do Setor de TI para que esta tome as providências cabíveis.

Incidentes Envolvendo o Tratamento de Dados Pessoais

Art. 117. São considerados exemplos de Incidentes envolvendo o tratamento de dados pessoais que devem ser notificados:

I – o vazamento de dados pessoais;

II – a suspeita de vazamento de dados pessoais;

III – a invasão ou tentativa de invasão do banco de dados pessoais;

IV – o compartilhamento ou cópia indevidos de dados pessoais;

V – violações da Política de Segurança da Informação da **PATRUS** envolvendo dados pessoais.

Art. 118. Qualquer incidente envolvendo o tratamento de dados pessoais deve ser comunicado imediatamente pelo Canal de Denúncias, que vai reportá-lo ao Encarregado pelo tratamento de dados pessoais e ao Comitê de Proteção de Dados Pessoais.

§ 1º Ao reportar o incidente envolvendo o tratamento de dados pessoais, o Usuário deve relacionar todos os detalhes, tais como mensagens da tela, comportamento estranho, não conformidade ou violações da Política de Segurança da Informação da **PATRUS**.

§ 2º O Usuário não deve tomar nenhuma ação própria para solucionar o Incidente envolvendo o tratamento de dados pessoais, mas reportá-lo imediatamente conforme disposto no *caput* deste artigo.

§ 3º Dependendo do grau de confidencialidade e sigilo requerido, o Usuário que enviou a notificação via e-mail pode não ser comunicado sobre as medidas tomadas para a solução do incidente

Art. 119. Em caso de incidentes envolvendo o tratamento de dados pessoais, o processo de contingenciamento disposto no Anexo I desta Política de Segurança deve ser observado.

CAPÍTULO 12 – NORMA DE INFRAÇÕES E PENALIDADES

Art. 120. A ação, a omissão ou a conivência de colaboradores e membros da Diretoria que impliquem desobediência ou inobservância das disposições desta Política de Segurança da Informação sujeitam o infrator às sanções abaixo descritas:

I – advertência por escrito;

II – suspensão não remunerada, conforme a legislação trabalhista, se colaborador for, ou suspensão;

III – demissão por justa causa, se colaborador;.

Parágrafo único - Colaboradores são considerados aqueles que mantêm vínculo trabalhista com a **PATRUS**, conceito que, para fins desta Política, se aplica à Diretoria.

Art. 121. O disposto neste capítulo não substitui a aplicação de sanções cíveis ou penais definidas na legislação pertinente.

ANEXO I – PLANO DE RESPOSTA A INCIDENTES ENVOLVENDO O TRATAMENTO DE DADOS PESSOAIS

Em geral, uma resposta ao vazamento de dados deve seguir quatro passos: contenção, avaliação, notificação e revisão. Os três primeiros passos (conter, avaliar e notificar) devem ser executados simultaneamente ou em rápida sucessão.

Passo 0 – Confirmação

Uma vez que o colaborador suspeitar que um vazamento de dados e/ou informação confidencial tenha ocorrido, ele deve imediatamente alertar seu Gestor e o Comitê de Proteção de Dados.

Os membros do Comitê, então, devem avaliar a situação e confirmar a existência de um incidente a fim de efetivamente iniciar o plano de contingenciamento.

Prazo: Até 24 horas

1º Passo – Contenção

Tendo certeza de que ocorreu um incidente, o Comitê deve notificar a Alta Direção para que esta, juntamente com ele, tome as medidas cabíveis.

No documento de notificação, devem constar:

- nome e informação de contato do indivíduo que descobriu o incidente;
- data e hora da descoberta do incidente;
- data, hora e local do incidente, se conhecidos;
- tipo de dados pessoais vazados (dados de colaboradores, dados de clientes, dados de terceiros);
- breve descrição do ocorrido;
- formato de armazenamento dos dados (papel, eletrônico, ambos);

que tipos de registros ou mídia o indivíduo acredita estarem envolvidos no vazamento;

- se o dispositivo ou informação vazada estavam protegidos por senha;
- se estava criptografada;
- se suspeita que dados pessoais identificados (nome, CPF, usernames e senhas, etc.) e/ou informação confidencial foram expostas;
- estimativa do volume de dados e/ou informações envolvidos;
- se já foi interrompido ou esgotado, ou se ainda há possibilidade de mais vazamentos.

Juntos, então, o Comitê e o indivíduo que identificou o vazamento (salvo tratando-se de denúncia anônima) devem fazer o possível para interromper, reverter ou limitar o vazamento – por exemplo, interrompendo a prática não autorizada, recuperando registros ou desligando o sistema que foi vazado. Não sendo prático o desligamento do sistema, ou se resultar em perda de evidência, revogar ou mudar os privilégios de acesso aos computadores, ou endereçar vulnerabilidades físicas e eletrônicas.

Nesta fase preliminar é vital, com base nas orientações do Comitê de Proteção de Dados, principalmente do representante jurídico, preservar as evidências em conformidade legal, de modo a identificar a causa e a autoria do vazamento e/ou permitir à

PATRUS endereçar todos os riscos representados aos titulares de dados envolvidos.

Prazo: Até 12 horas .

2º passo – Avaliação

Após a tentativa preliminar de contenção, o Comitê deve avaliar se o incidente representa algum risco de prejuízo grave aos titulares dos dados pessoais e à **PATRUS**.

O indivíduo que descobriu o incidente deve estar pronto para atuar junto ao Comitê nessa avaliação, caso necessário.

Caso se confirme o risco potencial de prejuízo aos titulares de dados e a **PATRUS**, o Comitê deve proceder ao terceiro passo do plano de contingenciamento. Não se confirmando tais suspeitas, é possível pular para o quarto passo.

O Encarregado (DPO) deve analisar as provas, as medidas extrajudiciais ou judiciais a serem tomadas e remeter o seu parecer ao responsável pelo poder diretivo da empresa para aprovação das medidas de enfrentamento sugeridas.

Prazo: Até 48 horas

3º passo – Notificação

Dependendo da abrangência do incidente, a autoridade controladora envolvida deve ser comunicada – por exemplo, Ministério Público, a Autoridade Nacional de Proteção de Dados – a respeito do incidente a fim de estabelecer laços de cooperação que podem mitigar possíveis prejuízos e penalidades.

Os titulares de dados afetados com o incidente também devem ser notificados, para que possam tomar as atitudes necessárias para resguardar e alertar pessoas próximas a eles de eventuais golpes e fraudes.

Prazo: Até 72 horas

4º passo – Revisão

O quarto passo envolve a revisão e a catalogação do relatório do incidente pelo Comitê e as tomadas de decisão para prevenir novos vazamentos da mesma natureza.

SÃO PAULO
Avenida Paulista 1079, Torre João Salem, 8º andar - São Paulo - SP
55 11 99502-8128

BELO HORIZONTE
Avenida Afonso Pena, 4273, 4º andar - Belo Horizonte - MG
55 31 3318-1414

BRASÍLIA
SCS, Quadra 09, Bloco C, Torre C, 10º andar - Comercial Sul, Brasília
55 61 99622-8128

ANEXO II – LISTA DE PROCEDIMENTOS OPERAÇÃO PADRÃO DA PATRUS

CÓDIGO	NOME
POP-D-TI-010	REDE – Política de TI
POP-D-TI-016	REDE – Criar Usuário de Rede
POP-D-TI-020	REDE – Criação de Usuário de E-mail
POP-D-TI-021	REDE – Administração de Banco de Dados/Rotina de Backup
POP-D-TI-026	REDE – Criar Usuários no MV Sistemas
POP-D-TI-072	REDE – Manutenção (Preventiva e Corretiva) do Ambiente de TI