POLÍTICA

GRUPO VOETUR

VTCLOG

VTC.LGPD.PLC.02 | Política de segurança da informação

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign	juciele.nogueira@voetur.com.br Assinado Juciele de Sousa Moura Nogueira D4Sign	assinatura@vtclog.com.br Assinado Raphael Reis de Sa D4Sign
Renato Salles Encarregado de Dados	Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	Juciele Nogueira Coordenadora de SGI	Raphael Sá CEO

SUMÁRIO

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign	juciele.nogueira@voetur.com.br Assinado Juciele de Sousa Moura Nogueira D4Sign	assinatura@vtclog.com.br Assinado Raphael Reis de Sá D4Sign
Renato Salles Encarregado de Dados	Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	Juciele Nogueira Coordenadora de SGI	Raphael Sá CEO

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign	juciele.nogueira@voetur.com.br Assinado Juciele de Sousa Moura Nogueira D4Sign	assinatura@vtclog.com.br Assinado Raphael Reis de Sa D4Sign
Renato Salles Encarregado de Dados	Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	Juciele Nogueira Coordenadora de SGI	Raphael Sá CEO

1. INTRODUÇÃO

A VTCLOG tem, na informação e nos dados, dois de seus principais ativos, devendo ambos ser adequadamente utilizados e protegidos contra riscos, ameaças, violações, acessos não autorizados e danos. É imprescindível, portanto, a adoção de condutas, normas e procedimentos padronizados que tenham como objetivo garantir a proteção dos três aspectos básicos da segurança da informação: **confidencialidade, integridade e disponibilidade**.

2. OBJETIVO

Esta política de segurança da informação tem por objetivo possibilitar o gerenciamento da segurança na VTCLOG, estabelecendo regras e padrões para proteção da informação. A política possibilita manter a confidencialidade, garantir que a informação não seja alterada ou perdida e permitir que os dados estejam disponíveis quando for necessário.

3. DEFINIÇÕES E SIGLAS

- **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;
- **Dado pessoal:** informação relacionada a pessoa natural identificada ou identificável;
- **Dado pessoal sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso,

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign	juciele.nogueira@voetur.com.br Assinado Juciele de Sousa Moura Nogueira D4Sign	assinatura@vtclog.com.br Assinado Raphael Reis de Sa D4Sign
Renato Salles Encarregado de Dados	Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	Juciele Nogueira Coordenadora de SGI	Raphael Sá CEO

filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

- **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;
- **Informação:** dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
- **Integridade:** propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- **Segurança da informação:** ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
- **Titular do dado:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
- **Ameaça:** causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

4. DIRETRIZES GERAIS

4.1. PRINCÍPIOS

As ações adotadas pelo setor de segurança da informação devem seguir, além do princípio da boa-fé, os seguintes princípios básicos:

I. Disponibilidade, integridade, confidencialidade e autenticidade das informações;

II. Continuidade dos processos e serviços essenciais para o funcionamento da VTCLOG.

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign Renato Salles Encarregado de Dados	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	juciele.nogueira@voetur.com.br Assinado Juciele de Sousa Moura Nogueira D4Sign Juciele Nogueira Coordenadora de SGI	assinatura@vtclog.com.br Assinado Raphael Reis de Sa D4Sign Raphael Sá CEO

III. Respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade;

IV. Responsabilidade do usuário de informação pelos atos que comprometam a segurança dos ativos de informação;

V. Conformidade das normas e das ações de segurança da informação com a legislação regulamentos aplicáveis; e

VI. Educação e comunicação como alicerces fundamentais para o fomento da cultura e segurança da informação.

VII. Simplicidade dos controles. A complexidade aumenta a chance de erros, portanto, todos os controles de segurança deverão ser simples e objetivos.

4.2. GESTÃO DA SEGURANÇA DA INFORMAÇÃO

A Gestão de segurança da informação possui uma estrutura definida dentro da VTCLOG, sendo ela:

I. Alta Direção;

II. Comitê de Segurança e Privacidade de Dados;

III. Encarregado pelo tratamento de dados (DPO);

IV. Gestor de Tecnologia da Informação;

V. Equipe de prevenção e tratamento de dados pessoais;

VI. Usuários de informação.

Cada um dos agentes que compõem a Gestão de segurança possui papel fundamental na estrutura da VTCLOG, sendo que a participação de todos é o que irá assegurar o sucesso desta política e do sistema de gestão e proteção de dados.

4.2.1. Alta Direção

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign Renato Salles Encarregado de Dados	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	juciele.nogueira@voetur.com.br Assinado Juciele de Sousa Moura Nogueira D4Sign Juciele Nogueira Coordenadora de SGI	assinatura@vtclog.com.br Assinado Raphael Reis de Sa D4Sign Raphael Sá CEO

A Alta Direção, formada pelos administradores e Sócios da VTCLOG é peça fundamental na estruturação do sistema de gestão de segurança de dados, cabendo a ela:

I.Fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação da VTCLOG, bem como com o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados;

II. Formalizar e aprovar as Políticas necessárias para o bom funcionamento do sistema de gestão de segurança da informação, bem como suas alterações e atualizações;

III. Deliberar sobre o objeto, a composição e o funcionamento do Comitê de Segurança e Privacidade de Dados, bem como deliberar sobre qualquer alteração a ser feita no Regimento interno do comitê.

4.2.2. Comitê de Segurança e Privacidade de Dados

O Comitê é um órgão colegiado de assessoramento e orientação à Alta Direção da VTCLOG, tendo sido por esta criado, visando o planejamento, coordenação e supervisão das atividades de segurança da informação e privacidade de dados pessoais.

O Comitê é independente às demais áreas/equipes internas, estando subordinado somente à Alta Direção da VTCLOG.

O Comitê de Segurança e Privacidade de dados da VTCLOG será formado por, no mínimo, 3 (três) e, no máximo, 6 (seis) membros efetivos, além de outros 3 (três) suplentes, todos profissionais de reputação incontestável, indicados pela Alta Direção.

Compete ao comitê as seguintes atividades:

I.Avaliar e monitorar as exposições de risco da VTCLOG, acompanhando e supervisionando o processo de gerenciamento de riscos relacionados aos dados que a empresa gere;

II. Avaliar as ocorrências de possíveis vazamentos de dados e solicitações dos titulares de dados recebidas por Canal interno ou qualquer outro meio;

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign Renato Salles Encarregado de Dados	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	juciele.nogueira@voetur.com.br Assinado Juciele de Sousa Moura Nogueira D4Sign Juciele Nogueira Coordenadora de SGI	assinatura@vtclog.com.br Assinado Raphael Reis de Sa D4Sign Raphael Sá CEO

III. Acompanhar seus administradores, colaboradores e prestadores de serviços quanto ao cumprimento das normas internas de segurança da informação, exigindo e zelando pela sua fiel execução;

IV. Emitir recomendações sobre situações específicas relacionadas ao tratamento de dados;

V. Submeter à Alta Direção suas recomendações sobre questões de sua competência e reportar suas atividades periodicamente;

VI. Auxiliar o DPO em eventuais alterações nas políticas e procedimentos internos relacionados à gestão de dados.

4.2.3. Encarregado pelo tratamento de dados (DPO)

O Encarregado pelo tratamento de dados (DPO) será indicado pela VTCLOG, após passar por análise das áreas pertinentes e ser aprovado nos termos da Política de Nomeação. O Encarregado atuará como canal de comunicação entre a VTCLOG, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Caberá ao DPO:

I.Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências cabíveis;

II. Receber comunicações da ANPD e adotar providências;

III. Orientar os funcionários e os contratados da VTCLOG a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

IV. Auxiliar a VTCLOG na produção dos Relatórios de Impacto à Proteção de Dados Pessoais, tendo em vista que esta é uma obrigação do controlador;

V. Participar do comitê de Segurança e Privacidade de Dados;

VI. Emitir comunicados e ministrar treinamentos sobre proteção de Dados;

VII. Produzir e atualizar Políticas internas;

VIII.Responder questionários e auditorias sobre a proteção de dados pessoais;

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign Renato Salles Encarregado de Dados	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	juciele.nogueira@voetur.com.br Assinado Juciele de Sousa Moura Nogueira D4Sign Juciele Nogueira Coordenadora de SGI	assinatura@vtclog.com.br Assinado Raphael Reis de Sa D4Sign Raphael Sá CEO

IX. Atuar junto à ANPD em defesa dos interesses da VTCLOG em eventuais processos administrativos;

X. Executar as demais atividades pertinentes para que a organização esteja em conformidade com a Lei Geral de Proteção de Dados.

4.2.4. Gestor de Tecnologia da Informação

Além de suas atividades naturais, compete ao gestor de TI:

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. Auxiliar o DPO em quesitos técnicos relacionados à Segurança da informação;

III. Se necessário, disponibilizar membros de sua equipe para auxiliar a equipe de segurança da informação.

4.2.5. Equipe de prevenção e tratamento dos dados pessoais

Equipe de apoio ao comitê de segurança e privacidade de dados a ser criada com profissionais de diferentes áreas, visando garantir a segurança da informação e a conformidade com a LGPD.

4.2.6. Usuários da informação

Os usuários da informação são todos aqueles que, em virtude de suas atividades, possuem contato direto com dados tratados pela VTCLOG.

Compete aos usuários de Informação conhecer, cumprir e fazer cumprir esta Política e às demais Normas e Políticas específicas de segurança da informação da VTCLOG.

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign	juciele.nogueira@voetur.com.br Assinado Juciele de Sousa Moura Nogueira D4Sign	assinatura@vtclog.com.br Assinado Raphael Reis de Sa D4Sign
Renato Salles Encarregado de Dados	Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	Juciele Nogueira Coordenadora de SGI	Raphael Sá CEO

4.3. DIRETRIZES GERAIS DE SEGURANÇA DA INFORMAÇÃO

As diretrizes expostas a partir deste momento constituem os principais pilares da Gestão de Segurança da Informação da VTCLOG, norteando a elaboração das demais políticas e procedimentos internos.

4.3.1. Comportamentos seguros e esperados de nossos colaboradores

Independentemente do meio ou da forma em que se encontre, a informação está presente no dia a dia de todos que operam em nome da VTCLOG. Portanto, é fundamental que seja adotado comportamento seguro e condizente com o objetivo de proteger os ativos informacionais da empresa, com destaque para os seguintes itens:

I. Todos os colaboradores e prestadores de serviços devem assumir atitude proativa e engajada no que diz respeito à proteção das informações da VTCLOG;

II. Todos que atuam em nome da VTCLOG devem compreender as ameaças externas e internas que podem afetar a segurança da informação na empresa, tais como vírus de computador, interceptação de mensagens eletrônicas, bem como outros artifícios frequentemente utilizados para a roubar senhas e obter acesso a sistemas de informação;

III. Todos os recursos de informação devem ser projetados e utilizados para a consecução dos objetivos e finalidades específicos da VTCLOG. É vedada a utilização desses recursos para fins particulares ou distintos do original;

IV. Toda informação produzida ou recebida pelos colaboradores, terceirizados, fornecedores e prestadores de serviço, em razão da função exercida e/ou atividade profissional contratada, no âmbito da VTCLOG, é de propriedade da empresa.

V. Cada usuário é responsável pela segurança das informações dentro da VTCLOG;

VI. Todo tipo de acesso à informação da VTCLOG que não for explicitamente autorizado é proibido;

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign Renato Salles Encarregado de Dados	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	juciele.nogueira@voetur.com.br Assinado Juciele de Sousa Moura Nogueira D4Sign Juciele Nogueira Coordenadora de SGI	assinatura@vtclog.com.br Assinado Raphael Reis de Sa D4Sign Raphael Sá CEO

VII. As senhas de usuário são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros, anotadas em papel ou em sistema visível ou de acesso não protegido;

VIII. É vedada a alteração, supressão ou exclusão de qualquer informação por pessoa não autorizada e sem autorização;

IX. Qualquer tipo de dúvida sobre a Política de Segurança da Informação e seus Enunciados Normativos deve ser imediatamente esclarecida com o DPO.

4.3.2. Segurança de dados físicos

Apesar da VTCLOG estar buscando uma digitalização completa dos dados, ainda existem diversas informações físicas, sendo necessária a proteção do ambiente onde estes dados estiverem.

O ambiente onde estes dados serão armazenados deverá prevenir perda, dano ou comprometimento dos ativos, bem como contemplar, quando for o caso, medidas de segurança contra roubo, fogo, explosivos, fumaça, água, poeira, umidade e fungos, roedores e insetos, curto-circuito e outros danos elétricos, vandalismo, sabotagem, entre outros.

Além disso, o acesso as áreas que possuem grande quantidade de dados devem ser controladas:

I. Áreas cuja natureza ou o manuseio de documentos e a utilização dos recursos de processamento da informação não exijam proteção são consideradas áreas de acesso livre;

II. Áreas que abriguem em seu interior documentos, processos, recursos de processamento da informação ou reuniões e eventos de caráter reservado devem ser consideradas áreas de acesso restrito;

III. A localização das áreas de acesso restrito, bem como a sua capacidade de resistência a acessos não autorizados devem ser adequados ao grau de confidencialidade de documentos e informações existentes em seu interior;

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign Renato Salles Encarregado de Dados	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	juciele.nogueira@voetur.com.br Assinado Juciele de Sousa Moura Nogueira D4Sign Juciele Nogueira Coordenadora de SGI	assinatura@vtclog.com.br Assinado Raphael Reis de Sa D4Sign Raphael Sá CEO

IV. Assuntos confidenciais e de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais, entre outros).

V. Os dados digitais que forem impressos e se tornarem físicos NÃO PODEM ser mantidos em locais públicos com amplo acesso, devendo ser guardados em ambiente adequado e, se for o caso, destruídos imediatamente após a utilização.

4.3.3. Segurança dos dados digitais e controle de acessos.

A VTCLOG, agindo em conformidade com seu programa de ESG tem buscado diminuir cada vez mais o uso de papel, migrando os dados para o meio digital. Contudo, para que isso ocorra de maneira segura, é necessário desenvolver um conjunto de procedimentos, recursos e meios de conceder ou bloquear o acesso ao uso de informações e dados pertencentes a VTCLOG.

Diversas ferramentas podem ser usadas visando atingir esse objetivo, na VTCLOG, para que apenas pessoas autorizadas possam acessar determinadas informações, existe a Gestão de Acesso (conjunto de processos que controlam quem pode acessar determinado dado) e os Logs de acesso (registros de todas as atividades que ocorrem em um sistema computacional).

Além dessas, outras ferramentas também são utilizadas para dar maior robustez a segurança de informações, como o uso de sistemas baseados em papéis (Role-Based Access Control – RBAC). Esse modelo permite que os acessos sejam concedidos com base nas funções desempenhadas pelos colaboradores dentro da organização, assegurando que cada usuário tenha acesso somente às informações estritamente necessárias ao desempenho de suas atividades. A adoção do princípio do menor privilégio é essencial para mitigar riscos de exposição indevida de dados e para manter a rastreabilidade de ações críticas em ambientes digitais.

É imprescindível a aplicação de políticas de autenticação reforçada, sobretudo para acessos remotos ou sistemas que lidam com dados sensíveis. Nesse cenário, destaca-se

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign Renato Salles Encarregado de Dados	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	juciele.nogueira@voetur.com.br Assinado Juciele de Sousa Moura Nogueira D4Sign Juciele Nogueira Coordenadora de SGI	assinatura@vtclog.com.br Assinado Raphael Reis de Sa D4Sign Raphael Sá CEO

a utilização da Autenticação Multifatorial (Multi-Factor Authentication – MFA), que exige a validação da identidade do usuário por meio de dois ou mais fatores distintos, como a utilização de usuário e senha ou uso de Tokens. Em relação à MFA:

I. Todos os colaboradores, prestadores de serviços e terceiros que acessam sistemas, plataformas e serviços de Tecnologia da Informação da VTCLOG devem utilizar a Autenticação Multifatorial (MFA) como camada adicional de segurança durante o processo de login.

II. A MFA deve ser configurada e mantida de acordo com as diretrizes definidas pelo setor de TI da VTCLOG, garantindo que somente usuários autorizados possam acessar as informações e sistemas críticos.

III. O não cumprimento da obrigatoriedade do uso de MFA resultará em bloqueio temporário do acesso ao sistema até que a configuração seja corrigida.

A combinação de RBAC e MFA contribui significativamente para o fortalecimento do sistema de segurança da informação da VTC, dificultando o acesso não autorizado, mesmo em casos de comprometimento de credenciais. A configuração e o monitoramento desses controles deverão estar sob responsabilidade da equipe de tecnologia da informação, com revisões periódicas para garantir sua efetividade e conformidade com os princípios da LGPD.

4.3.3.1. Criptografia

A criptografia é uma grande aliada da segurança da informação, e poderá ser utilizada para manter a confidencialidade, a autenticidade e a integridade das informações pertencentes a VTCLOG.

I. Os algoritmos e os métodos de criptografia utilizados devem se basear em padrões de mercado e utilizar apenas tecnologias aprovadas pelo Gestor de TI;

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign Renato Salles Encarregado de Dados	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	juciele.nogueira@voetur.com.br Assinado juciele de Sousa Moura Nogueira D4Sign Juciele Nogueira Coordenadora de SGI	assinatura@vtclog.com.br Assinado Raphael Reis de Sa D4Sign Raphael Sá CEO

II. Certificação digital e assinatura digital poderão ser utilizados como forma de garantir a segurança nas comunicações institucionais.

4.3.3.2. Internet, Intranet e proteção contra softwares maliciosos

Os colaboradores que tiverem acesso à Internet e Intranet deverão utilizar o acesso de forma ética e profissional, sempre priorizando a proteção dos ativos de informação da VTCLOG.

I. O uso de recursos e serviços de TI da empresa são restritos aos colaboradores e usuários externos credenciados e autorizados, sendo vedada a sua utilização fora dessas condições;

II. A VTCLOG poderá, a qualquer tempo e sem aviso prévio aos usuários, bloquear, restringir, filtrar, monitorar, capturar, controlar ou auditar todos os recursos e os serviços de TI no âmbito da empresa, estejam eles nas estações de trabalho ou nos servidores de rede, visando assegurar o cumprimento de suas Políticas internas;

III. É vedado o uso de recursos computacionais e de comunicação da VTCLOG para disseminação de conteúdo protegido por direitos autorais, ilegais, sabidamente falsos ou com discurso de ódio;

IV. É proibido, sob qualquer alegação ou pretexto, o uso de qualquer meio ou subterfúgio para burlar, fraudar, anular ou impedir a ação dos sistemas de segurança da informação implementados na VTCLOG;

V. Falhas de segurança da informação percebidas pelos usuários deverão ser comunicadas a equipe de TI imediatamente para que sejam tomadas as devidas providências.

No contexto da VTCLOG devem existir medidas de prevenção e detecção automática de softwares maliciosos, assim como programas de conscientização dos usuários. Os usuários devem ser orientados de que a prevenção é sempre a melhor solução.

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign Renato Salles Encarregado de Dados	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	juciele.nogueira@voetur.com.br Assinado Juciele de Sousa Moura Nogueira D4Sign Juciele Nogueira Coordenadora de SGI	assinatura@vtclog.com.br Assinado Raphael Reis de Sa D4Sign Raphael Sá CEO

I. Os Recursos de Tecnologia da Informação devem estar sempre munidos de soluções de detecção e bloqueio de programas de código malicioso, como, por exemplo, antispyware, programas antivírus;

II. A instalação e a configuração da solução de detecção e bloqueio de programas maliciosos somente devem ser realizadas pela equipe de TI;

III. Tais softwares devem ser atualizados constantemente, e sua execução deve ser agendada para ocorrer periodicamente;

IV. Qualquer mídia removível de origem duvidosa ou não autorizada deve ser avaliada quanto à presença de vírus ou outros softwares maliciosos antes de ser utilizada. Arquivos recebidos por correio eletrônico também devem ser inspecionados, sendo possível que a VTCLOG faça testes periódicos de *Phishing* para verificar se os funcionários estão atentos a possíveis programas maliciosos.

V. É vedada a instalação de softwares nos recursos computacionais da VTCLOG sem o prévio conhecimento e autorização da área responsável. Os usuários devem fazer uso apenas de softwares licenciados e homologados pela área de TI.

4.3.3.3. E-mail e Spam

O e-mail é uma ferramenta de trabalho disponibilizada para a grande maioria dos funcionários da VTCLOG com o objetivo de execução dos serviços e maior facilidade na comunicação. Dessa forma, ele deverá ser utilizado somente para fins corporativos e relacionados às atividades do colaborador, sendo vedada a sua utilização para tratar de assuntos de cunho pessoal.

A VTCLOG também possui um sistema de controle AntiSpam, que são mensagens eletrônicas enviadas em massa e não solicitas, facilitando que o e-mail sirva única e exclusivamente para fins profissionais.

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign	juciele.nogueira@voetur.com.br Assinado Juciele de Sousa Moura Nogueira D4Sign	assinatura@vtclog.com.br Assinado Raphael Reis de Sa D4Sign
Renato Salles Encarregado de Dados	Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	Juciele Nogueira Coordenadora de SGI	Raphael Sá CEO

4.3.3.4. Backup

Em relação aos Backups (cópias de segurança) realizados pela VTCLOG, deverão ser observadas as seguintes diretrizes gerais:

I. A realização do backup institucional consistirá no armazenamento da cópia dos dados contidos nos computadores servidores da VTCLOG. A realização de backup dos dados contidos nas estações de trabalho é de responsabilidade de cada usuário. A empresa não se responsabiliza por nenhum conteúdo presente nas máquinas utilizadas pelos colaboradores;

II. Todos os documentos pertinentes às atividades institucionais da VTCLOG deverão ser armazenados nos servidores da adequados. Tais arquivos, se gravados apenas localmente nos computadores dos usuários, não serão incluídos na rotina de backup e poderão ser perdidos caso ocorra uma falha na máquina, situação em que a responsabilidade será inteiramente do usuário, podendo ele ser responsabilizado por quaisquer prejuízos a VTCLOG;

III. Arquivos pessoais e/ou não pertinentes às atividades institucionais da VTCLOG, tais como fotos, músicas, vídeos, entre outros, não deverão ser copiados ou movidos para os drives de rede. Caso identificados, esses arquivos poderão ser excluídos sem a necessidade de comunicação prévia ao usuário;

IV. É vedado o armazenamento de informações corporativas, tais como bases de dados, arquivos, ou demais documentos em locais inadequados, como serviços de armazenamento em nuvem pessoais, computadores pessoais ou servidores de prestadores de serviço, salvo nos casos em que tais práticas sejam previamente autorizadas e apenas quando necessárias ao fiel cumprimento do dever institucional

As demais disposições técnicas referentes aos Backups da VTCLOG serão abordadas em Política específica sobre o tema, devendo este documento ser conhecido principalmente pela equipe chefiada pelo Gestor de TI, responsável por verificar o cumprimento da política com auxílio da Sistema de Gestão Integrada (SGI).]

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign Renato Salles Encarregado de Dados	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	juciele.nogueira@voetur.com.br Assinado juciele de Sousa Moura Nogueira D4Sign Juciele Nogueira Coordenadora de SGI	assinatura@vtclog.com.br Assinado Raphael Reis de Sa D4Sign Raphael Sá CEO

4.3.3.5. Sanitização de ativos de tecnologia

A sanitização de ativos de tecnologia da informação é uma etapa fundamental no ciclo de vida da informação na VTC, especialmente no contexto da proteção de dados pessoais. Tal procedimento visa garantir que, ao serem descontinuados ou realocados, dispositivos e sistemas não mantenham qualquer vestígio de dados sensíveis, confidenciais ou estratégicos da empresa.

A sanitização deverá ser feita nos Hardwares e Softwares de propriedade da VTC. Este processo deverá ser implementado pela equipe de TI, devendo haver um processo formal e documentado de desinfecção, limpeza lógica e descarte seguro de equipamentos de TI que estejam obsoletos, com defeito ou fora de uso (ex.: HDs, SSDs, computadores, servidores, impressoras com armazenamento, etc.).

Esse processo deve prever:

I. A remoção permanente dos dados por meio de ferramentas especializadas de limpeza;

II. A destruição física dos dispositivos, quando necessário, por meio de trituração, desmagnetização ou incineração certificada;

III. O registro completo do processo, contendo data, equipamento, destino e responsáveis técnicos;

IV. O envolvimento da equipe de TI e, quando necessário, de empresas especializadas com certificação para descarte ecológico e seguro de equipamentos eletrônicos, seguindo os princípios de ESG adotados pela VTC.

A sanitização também deve ocorrer nos softwares, sistemas e bases de dados utilizados, sempre que forem desativados, substituídos ou migrados. A sanitização deve ser adotada para garantir a remoção segura e definitiva das informações sensíveis neles contidas.

Essas medidas devem incluir:

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign Renato Salles Encarregado de Dados	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	juciele.nogueira@voetur.com.br Assinado Juciele de Sousa Moura Nogueira D4Sign Juciele Nogueira Coordenadora de SGI	assinatura@vtclog.com.br Assinado Raphael Reis de Sa D4Sign Raphael Sá CEO

I. A documentação formal dos procedimentos de desinstalação e descontinuidade dos sistemas;
II. A eliminação completa de registros, logs e arquivos temporários ou residuais, especialmente aqueles que contenham dados pessoais, de clientes, colaboradores ou fornecedores;
III. A revogação imediata de acessos, chaves de API, autenticações remotas e credenciais associadas ao software;
IV. O encerramento formal do ciclo de vida do sistema.

O processo de sanitização de software e hardware deverá ser acompanhado pela equipe de TI, sob a supervisão do Gestor de Tecnologia da Informação.

4.3.3.6. Gestão de riscos e melhoria contínua

A gestão de riscos relacionados à segurança da informação será tratada de forma estruturada e permanente no âmbito da VTC, com base nas diretrizes da norma ISO/IEC 27001 e demais marcos regulatórios aplicáveis, como a Lei Geral de Proteção de Dados (LGPD).

A gestão de riscos deverá contemplar:

I. A análise periódica dos riscos associados ao tratamento de dados pessoais e ativos de informação;
II. A identificação de ameaças e vulnerabilidades que possam impactar a confidencialidade, integridade, disponibilidade e autenticidade da informação;
III. A avaliação do impacto e da probabilidade de ocorrência dos riscos identificados, utilizando metodologias quantitativas, qualitativas ou híbridas;
IV. A classificação dos riscos conforme níveis de aceitabilidade previamente definidos pela organização;

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign Renato Salles Encarregado de Dados	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	juciele.nogueira@voetur.com.br Assinado juciele de Sousa Moura Nogueira D4Sign Juciele Nogueira Coordenadora de SGI	assinatura@vtclog.com.br Assinado Raphael Reis de Sa D4Sign Raphael Sá CEO

V. A implementação de medidas de tratamento, priorizando ações de mitigação, transferência, aceitação ou eliminação do risco, com planos de ação específicos, prazos e responsáveis.

O Comitê de Segurança e Privacidade de Dados, em conjunto com a área de Tecnologia da Informação e o DPO, será responsável por validar a metodologia de avaliação de riscos e supervisionar sua execução periódica.

A gestão de risco poderá impactar a reformulação de procedimentos internos sempre que necessário para mitigar os fatores identificados, devendo este processo ser feito anualmente pela equipe de TI, quando envolver ativos e dados em geral e pelo DPO quando se tratar de dados pessoais.

4.4. INCIDENTES COM DADOS

Os incidentes envolvendo dados será abordado em Política específica, contudo é essencial ter em mente as seguintes premissas:

I. Os incidentes deverão ser investigados, estudados e sanados, de forma a preservar disponibilidade, integridade, confidencialidade e autenticidade da informação;

II. Todos os incidentes notificados ou detectados deverão ser registrados, com a finalidade de assegurar registro histórico das atividades desenvolvidas;

III. Caberá aos usuários comunicarem a seus supervisores, que por sua vez notificará o comitê de segurança e privacidade de dados sobre as falhas e os incidentes de que tomem conhecimento;

IV. No caso de indícios de ilícitos criminais, o comitê de segurança e privacidade de dados, junto com o comitê de ética, terão como dever, sem prejuízo de suas demais atribuições, acionar as autoridades competentes para a adoção dos procedimentos legais cabíveis;

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign	juciele.nogueira@voetur.com.br Assinado Juciele de Sousa Moura Nogueira D4Sign	assinatura@vtclog.com.br Assinado Raphael Reis de Sa D4Sign
Renato Salles Encarregado de Dados	Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	Juciele Nogueira Coordenadora de SGI	Raphael Sá CEO

V. Eventuais comunicações de incidente à ANPD serão debatidas e decididas pelo comitê de segurança e privacidade de dados.

5.4 CONSEQUÊNCIAS DISCIPLINARES DECORRENTES DA VIOLAÇÃO DESTA POLÍTICA

No caso de ser verificada violação a esta Política, incidirão sobre o infrator medidas disciplinares, a serem estabelecidas de acordo com a sua função, a natureza da violação, eventual reincidência e impactos à empresa.

As seguintes medidas poderão ser adotadas, sem prejuízo da responsabilização civil e criminal aplicáveis:

- Advertência verbal;
- Advertência escrita;
- Suspensão;
- Readequação das atividades;
- Demissão;
- Rescisão contratual.

5. ANEXOS

- Não aplicável;

6. NÃO CONFORMIDADE E/OU OCORRÊNCIAS

Quaisquer desvios dos processos descritos neste procedimento em questão serão avaliados pelo Sistema de Gestão Integrado e/ou Garantia da Qualidade para abertura de

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign Renato Salles Encarregado de Dados	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	juciele.nogueira@voetur.com.br Assinado juciele de Sousa Moura Nogueira D4Sign Juciele Nogueira Coordenadora de SGI	assinatura@vtclog.com.br Assinado Raphael Reis de Sa D4Sign Raphael Sá CEO

não conformidades ou ocorrências. Os gestores das áreas envolvidas devem garantir o cumprimento deste procedimento e serão responsáveis por parte do conjunto de ações necessárias para resolução de eventuais não conformidades ou ocorrências que tenham sido abertas provenientes do descumprimento do processo.

Todo e qualquer colaborador, ao identificar uma não conformidade, deve de imediato comunicar ao superior que adotará as ações para garantir que as causas sejam identificadas e tratadas e ações de melhoria possam ser propostas.

7. SEGURANÇA DA INFORMAÇÃO

A segurança da informação de todos os processos do GRUPO VOETUR é balizada por esta política, sendo os riscos identificados e monitorados por meio do Software RISK do Qualyteam e/ou pela matriz de risco, contemplando as seguintes etapas: identificação, avaliação, tratamento, monitoramento e comunicação.

8. REFERÊNCIAS

- ISO 9001:2015 – Sistema de Gestão da Qualidade.
- ISO 27001:2022 – Tecnologia da informação – Técnicas de Segurança – Sistemas de Gestão da Segurança da Informação.
- Resolução CD/ANPD nº 18, de 16 de julho de 2024.
- ABNT NBR ISO/IEC 27002:2022 Tecnologia da Informação-Técnicas de Segurança – Código de Prática para controles de segurança da informação;

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign Renato Salles Encarregado de Dados	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	juciele.nogueira@voetur.com.br Assinado Juciele de Sousa Moura Nogueira D4Sign Juciele Nogueira Coordenadora de SGI	assinatura@vtclog.com.br Assinado Raphael Reis de Sa D4Sign Raphael Sá CEO

9. HISTÓRICO DE REVISÕES

VERSÃO	DATA	ITENS REVISADOS
00	03/04/2025	Primeira publicação do documento.

Elaboração	Verificação		Aprovação
renato.filho@vtclog.com.br Assinado Renato Salles D4Sign Renato Salles Encarregado de Dados	victor.ramalho@voetur.com.br Assinado Victor Vargas Ramalho D4Sign Victor Ramalho Presidente do Comitê de Segurança e Privacidade de Dados	juciele.nogueira@voetur.com.br Assinado Juciele de Sousa Moura Nogueira D4Sign Juciele Nogueira Coordenadora de SGI	assinatura@vtclog.com.br Assinado Raphael Reis de Sa D4Sign Raphael Sá CEO

VTC LGPD PLC 02 - Politica de Segurança da Informação pdf

Código do documento c71f0107-55f4-4448-9e5e-e83d6570b03b

Assinaturas

Renato Luqueiz Salles FIlho
renato.filho@vtclog.com.br
Assinou como Encarregado de Dados

Victor Vargas Ramalho
victor.ramalho@voetur.com.br
Assinou como Presidente do comitê de Segurança e Privacidade de Dados

Juciele de Sousa Moura Nogueira.
juciele.nogueira@voetur.com.br
Assinou como Coordenadora de SGI

Raphael Reis de Sa
assinatura@vtclog.com.br
Assinou como C.E.O

Eventos do documento

04 Apr 2025, 11:17:20
Documento c71f0107-55f4-4448-9e5e-e83d6570b03b **criado** por SERVIÇOS - ASSINATURA ELETRÔNICA (03eafde7-d827-4056-beec-336f45ab5c12). Email:servicos.assinaturaeletronica@voetur.com.br. - DATE_ATOM: 2025-04-04T11:17:20-03:00

04 Apr 2025, 11:31:58
Assinaturas **iniciadas** por SERVIÇOS - ASSINATURA ELETRÔNICA (03eafde7-d827-4056-beec-336f45ab5c12). Email: servicos.assinaturaeletronica@voetur.com.br. - DATE_ATOM: 2025-04-04T11:31:58-03:00

04 Apr 2025, 11:59:29
VICTOR VARGAS RAMALHO **Assinou como Presidente do comitê de Segurança e Privacidade de Dados** - Email: victor.ramalho@voetur.com.br - IP: 186.193.10.34 (pool-186-193-10-34.wixx.com.br porta: 19398) - Geolocalização: -15.792234434863124 -47.89347311090702 - Documento de identificação informado: 009.136.671-29 - DATE_ATOM: 2025-04-04T11:59:29-03:00

04 Apr 2025, 15:16:52
SERVIÇOS - ASSINATURA ELETRÔNICA (03eafde7-d827-4056-beec-336f45ab5c12). Email: servicos.assinaturaeletronica@voetur.com.br. **ALTEROU** o signatário **renato.filho@voetur.com.br** para **renato.filho@vtclog.com.br** - DATE_ATOM: 2025-04-04T15:16:52-03:00

24 páginas - Datas e horários baseados em Brasília, Brasil
Sincronizado com o NTP.br e Observatório Nacional (ON)
Certificado de assinaturas gerado em 04 de April de 2025, 16:59:36

04 Apr 2025, 15:36:42
RENATO LUQUEIZ SALLES FILHO **Assinou como Encarregado de Dados** - Email: renato.filho@vtclog.com.br - IP: 177.69.47.65 (177-069-047-065.static.ctbctelecom.com.br porta: 4436) - Geolocalização: -15.7964 -47.8947 - Documento de identificação informado: 055.844.351-63 - DATE_ATOM: 2025-04-04T15:36:42-03:00

04 Apr 2025, 16:28:55
RAPHAEL REIS DE SA **Assinou como C.E.O** (79cea41c-6454-4e7f-8b53-a539800f991f) - Email: assinatura@vtclog.com.br - IP: 177.69.47.65 (177-069-047-065.static.ctbctelecom.com.br porta: 12136) - Geolocalização: -15.791576 -47.893724 - Documento de identificação informado: 026.980.281-90 - DATE_ATOM: 2025-04-04T16:28:55-03:00

04 Apr 2025, 16:56:29
JUCIELE DE SOUSA MOURA NOGUEIRA. **Assinou como Coordenadora de SGI** (79870a25-3ce4-45c5-9263-e8b53b0e3046) - Email: juciele.nogueira@voetur.com.br - IP: 177.30.136.161 (161.136.30.177.isp.timbrasil.com.br porta: 9336) - Documento de identificação informado: 023.447.033-06 - DATE_ATOM: 2025-04-04T16:56:29-03:00

Hash do documento original
(SHA256):8b86d4b6a21689e9e8e8be8ce3896950abb46f8b7db3be59c534629382aa3456
(SHA512):e829c59b865e938915803184f8fb0f23c9a6626980955309aacb31c645957cdf3cd6e4b3e0ee15c2d19fa2be4d33b5f75de31e4463dd081edb20abc23fa19346

Esse log pertence **única** e **exclusivamente** aos documentos de HASH acima

Esse documento está assinado e certificado pela D4Sign
Integridade certificada no padrão ICP-BRASIL
Assinaturas eletrônicas e físicas têm igual validade legal, conforme **MP 2.200-2/2001** e **Lei 14.063/2020**.