POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA TERCEIROS

Elaborado por:	Revisado por:	**Aprovado por:**
Felipe de Lara Analista Segurança Cibernética	Rafaela Alcobaça Analista de Governança de TI	Marcos Faria Diretor de Estrutura de TI
Pedro Mota Analista Segurança Cibernética	Fernanda Kleis Especialista de Governança de TI	Luiz Fernando Borrego Diretor Executivo de TI
	Flavia Segura Gerente de Governança de TI e Segurança da Informação	
	Lucas Correia Gerente de Segurança Cibernética	
	Camilla Rocha Vanzella Coordenadora de Suprimentos	
	Jéssica P. V. Ribeiro Advogada	

ÍNDICE

1. Objetivo

A informação é um dos elementos de negócio mais importantes para o Grupo GOL e, dessa forma, manter a sua confidencialidade, integridade e disponibilidade são fatores críticos para a Companhia. A **Política de Segurança da Informação para Terceiros** tem como objetivo principal estabelecer diretrizes claras e robustas para a proteção dos ativos de informação da Companhia, garantindo a confidencialidade, integridade e disponibilidade dos dados sob responsabilidade do Terceiro. Esta política serve como base para a definição de padrões, procedimentos e controles de segurança, alinhados às melhores práticas do mercado e à legislação aplicável, visando mitigar riscos, prevenir incidentes e assegurar a conformidade com os requisitos contratuais e regulatórios. Além disso, busca promover uma cultura de segurança da informação entre todos os envolvidos, reforçando a importância da proteção dos ativos como parte integrante das operações e da relação entre as Partes.

2. Alcance

Todas as empresas e indivíduos jurídicos que estabelecem contratos formais com a Companhia, se obrigam a cumprir os requisitos de Segurança da Informação aqui definidos. O cumprimento das diretrizes estabelecidas é fundamental para a efetiva relação de parceria firmada para atingir níveis adequados de proteção à informação.

3. Definições e Abreviaturas

Companhia: GOL LINHAS AÉREAS INTELIGENTES S.A e todas as suas empresas subsidiárias diretas e indiretas incluindo, sem se limitar, a GOL LINHAS AÉREAS S.A.

Contrato: Qualquer instrumento que gere direitos e obrigações para a Companhia incluindo, mas não se limitando a: contratos, aditivos, termos de acordo, cartas de intenção, distratos/termos de encerramento, notificações e documentos correlatos.

Gestor do Contrato: Diretor, gerente executivo, gerente ou coordenador da Companhia sendo colaborador integrante da Área Requisitante responsável pela solicitação de Contrato à Gerência Jurídica de Contratos.

Gerência Jurídica de Contratos: Gerência integrante da Diretoria Jurídica da Companhia, composta pelo Núcleo de Controle de Contratos e pelos Advogados.

Pessoa Jurídica: Designa uma entidade que detentora de direitos e obrigações e à qual se atribui personalidade jurídica, possuindo definição legal conforme Código Civil Brasileiro.

Terceiro: Um indivíduo, entidade, organização e/ou seus representantes que tenha negócios existentes e/ou pretendidos com a GOL. Isto inclui fornecedores, empreiteiros, consultores, potenciais ou existentes e parceiros.

4. Papéis e Responsabilidades

4.1 Diretor Executivo de TI

- Estabelecer a direção estratégica para a segurança da informação e garantir que os requisitos de segurança sejam integrados na estratégia geral da organização;
- Disponibilizar recursos para implementar e manter medidas de segurança adequadas relacionadas as contratações de terceiros;
- Assegurar que os recursos necessários para atendimento do processo de gestão de riscos de terceiros estão disponíveis (papéis e responsabilidades definidos, ferramentas disponíveis);
- Assumir a responsabilidade final pela segurança da informação e pela gestão de riscos associados a terceiros.

4.2 Segurança Cibernética

- Definir diretrizes de segurança da informação para terceiros, incluindo requisitos de segurança, padrões e procedimentos a serem seguidos;
- Avaliar as práticas de segurança de terceiros, incluindo fornecedores e contratados, para garantir que atendam aos padrões da organização;
- Monitorar o acesso de terceiros aos sistemas e recursos de TI da empresa e aplicar controles de acesso apropriados;
- Investigar e responder a incidentes de segurança relacionados a terceiros;

- Garantir que os funcionários que interagem com terceiros sejam devidamente treinados em questões de segurança da informação;
- Identificar e avaliar riscos relacionados à segurança da informação associados a terceiros sempre que necessário;
- Desenvolver estratégias para mitigar riscos e propor ações corretivas quando necessário;
- Analisar tecnicamente e previamente a confecção de Contrato jurídico as contratações da Companhia do viés de segurança da informação, assim como avaliar cláusulas e condições contratuais sempre que necessário;
- Apontar riscos identificados na contratação de terceiros do viés de segurança da informação, bem como pontuar necessidade de ajustes nos Contratos da Companhia a Gerência Jurídica de Contratos.

4.3 Governança de TI

- Verificar o cumprimento das políticas e padrões de segurança da informação;
- Acompanhar as práticas de terceiros em relação a regulamentações e padrões de segurança relevantes;
- Relatar descobertas e recomendações para a Diretoria de TI e a equipe de Segurança cibernética;
- Apoiar na revisão e publicação desse documento.

4.4 Gerência Jurídica de Contratos

- Receber e analisar juridicamente as demandas jurídicas da Companhia, incluindo sem se limitar aos Contratos;
- Direcionar para análise técnica e aprovação da área de Segurança Cibernética cláusulas e condições contratuais relacionadas à contratação de terceiros;
- Pontuar riscos jurídicos identificados nos Contratos relacionados à contratação de terceiros, para análise e aprovação do Gestor do Contrato;
- Analisar do viés jurídico incidentes de segurança da informação envolvendo

terceiros, sempre que acionada pelas áreas internas, especialmente pela área de segurança cibernética;

- Elaborar Contratos incluindo cláusulas de segurança da informação estabelecendo os direitos e responsabilidades das partes, sempre que o escopo contratual exija tal inclusão;
- Direcionar para avaliação técnica da área de Segurança Cibernética cláusulas contratuais existentes em Contratos de parceiros, fornecedores e clientes;
- Analisar do viés jurídico questões de segurança da informação sempre que acionada pelas áreas internas, especialmente pela área de segurança cibernética.

4.5 Área Contratante de Serviços de Fornecedores

- Garantir que os requisitos sejam claramente comunicados aos Terceiros antes da contratação e formalizados em contratos ou anexos específicos;
- Quando da contratação de fornecedores que tenham colaboradores que venham a acessar a rede interna e os dados da Companhia, a área contratante deverá garantir que todos sejam treinados dentro do Programa de Treinamento e Conscientização em Segurança da Informação da Companhia;
- Manter um canal de comunicação aberto e transparente com os Terceiros para tratar de questões relacionadas à segurança da informação.

4.6 Prestador de Serviços/ Fornecedores/Terceiros

- É de responsabilidade destes observar e seguir as orientações estabelecidas para o cumprimento da presente Política de Segurança da Informação para Terceiros;
- Todas as atividades executadas devem observar a legislação vigente e a normatização de órgãos e entidades reguladoras com relação à Segurança da Informação.

4.7 Diretoria de Gente e Cultura

- Realizar verificações de antecedentes e avaliações de risco ao contratar terceiros que terão acesso a informações confidenciais ou sistemas críticos;
- Gerenciar a documentação e registros relacionados a terceiros, incluindo acordos e certificações de treinamento.

5. Referências

ISO/IEC 27005:2019 Sistemas de Gestão de Segurança da Informação;

Manual de Suporte ao Fornecedor GOL (https://static.voegol.com.br/voegol/2021-07-19/manual-de-suporte-ao-fornecedor-GOL.pdf);

Cartilha Diretrizes de Conduta Terceiros na Relação com a GOL (https://static.voegol.com.br/voegol/2021-07-19/CartilhaDiretrizesdeCondutaTerceirosnaRelacaocomaGOL.pdf);

PO-SUP-MS-001 – Política de Aquisições da Companhia.

6. Considerações Gerais

Os terceiros/prestadores de serviços/fornecedores devem cumprir com todos os requisitos da legislação brasileira aplicáveis, e devem comprometer-se a seguir integralmente os pilares a seguir, baseados nas melhores práticas de segurança da informação:

- Governança de Segurança da Informação;
- Proteção de Dados;
- Gestão de Riscos;
- Gerenciamento de Contas e Acessos;
- Gestão de Ativos;
- Segurança nas Operações;
- Gerenciamento de Logs e Incidentes;
- Gerenciamento de Vulnerabilidades;

- Desenvolvimento Seguro;
- Segurança nas Comunicações;
- Segurança Física;
- Continuidade de Negócios e Gestão de Crise;
- Treinamento e Conscientização.

Ainda se comprometem a:

- Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada, mantendo a sua confidencialidade;
- Assegurar que os recursos colocados à sua disposição sejam utilizados apenas para as finalidades aprovadas pela Companhia;
- Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos;
- Garantir a continuidade do processamento das informações críticas de negócios;
- Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;
- Atender às leis – no que lhes for aplicável e inerente ao exercício da sua função - que regulamentam as atividades da Companhia e seu mercado de atuação;
- Comunicar a companhia quando houver incidentes de segurança da informação e que afete informações e/ou gere impacto para a GOL;
- Prestadores de Serviço/Fornecedores devem passar por processo de avaliação de Segurança da Informação, através de SelfAssessment de SI na pré-contratação, contratação ou periodicamente pós contratação.

7. Requisitos de Segurança da Informação de Terceiros nos ambientes da Companhia.

7.1.1 Acesso Lógico e Uso Aceitável

- O acesso lógico ao ambiente da rede interna da Companhia deverá ser solicitado pelo gestor responsável pela contratação, por meio da ferramenta de chamados ITSM. A solicitação será avaliada e aprovada de acordo com a necessidade, seguindo as diretrizes corporativas de Segurança da Informação e Governança de TI;
- Para terceiros/prestadores de serviço/fornecedores que precisam acessar o ambiente da Companhia remotamente, o gestor responsável pelo contrato deve providenciar acesso através de usuário único e individual com acesso a VPN, no qual somente poderá ter acesso aos recursos de trabalho e ambientes necessários para o desempenho de suas funções;
- É dever do gestor responsável pelo terceiro informar a validade do contrato de prestação de serviços no momento da solicitação do acesso, bem como solicitar a exclusão do acesso quando não houver mais necessidade;
- Os computadores de terceiros não podem ser conectados na rede interna da Companhia sem a aprovação prévia da TI, sendo que estes deverão estar protegidos por software antivírus/anti-malware e demais softwares devidamente licenciados;
- É proibido o acesso, download ou distribuição de qualquer conteúdo que viole direitos autorais e de propriedade dentro da rede da Companhia. Da mesma forma, não é permitido acesso ou distribuição de conteúdo pornográfico de qualquer natureza ou conteúdo que viole o Estatuto da Criança e Adolescente;
- Quando aplicável, o usuário e senha disponibilizado para o terceiro são de uso exclusivo e não podem ser divulgados ou compartilhados;
- O terceiro deve manter suas credenciais de acesso seguras, sendo de sua responsabilidade qualquer utilização indevida;
- É responsabilidade da empresa terceira comunicar qualquer desligamento de seus colaboradores para que eles tenham seus acessos devidamente cancelados no

ambiente da Companhia; e

- É proibido o compartilhamento de usuários e senhas entre os prestadores de serviços.

7.1.2 Notificação de Incidentes de Segurança da Informação

- Incidentes e não-conformidades de Segurança da Informação que sejam de conhecimento do terceiro devem ser imediatamente comunicados à Companhia ou ao gestor do contrato para que este realize o processo de notificação de incidente pelos meios formais;
- Uma vez aberto, o processo de triagem, análise, tratamento e resposta segue o mesmo fluxo dos incidentes internos da Companhia.

7.1.3 Segurança de Equipamentos

- Cada usuário é responsável pela proteção dos dispositivos físicos contendo informação da Companhia que estão sob sua guarda; e
- Cada usuário deve estar ciente que o uso de qualquer recurso de TI no ambiente da Companhia, ainda que de propriedade pessoal, está sujeito a vistoria, sempre que a lei local permitir.

7.1.4 Violação de Conduta

São consideradas violações à esta Política as seguintes situações, não se limitando a:

- Quaisquer ações ou situações que possam expor a Companhia à perda financeira, operacional e de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;
- Uso indevido de dados corporativos, divulgação não autorizada de informações, segredos comerciais ou outras informações sem a permissão expressa da Companhia;
- Uso de dados, informações, equipamentos, software, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos

reguladores da área de atuação da Companhia; e

- A não-comunicação imediata de quaisquer descumprimentos da Política.

8. Controles de Segurança no ambiente do terceiro

Ao identificar a necessidade, conforme critérios de avaliação de riscos de segurança da informação e cibernética dispostos no "PR-DTI-SC-015 - Procedimento Gestão de Riscos de Fornecedores", a área de Segurança Cibernética irá cadastrar o fornecedor em questão em ferramenta de verificação de riscos. A equipe de Segurança Cibernética então realizará a análise do fornecedor. Caso o mesmo não atinja o resultado mínimo para a prestação de seu serviço, ele será negado pelo time de Segurança Cibernética, até que implemente as melhorias necessárias geradas pelo plano de recomendações da plataforma.

8.1 Governança de Segurança da Informação

- O terceiro deve manter uma estrutura de governança de segurança da informação compatível com as melhores práticas de mercado, como ISO 27001 e NIST, garantindo a conformidade com regulamentações vigentes e requisitos contratuais estabelecidos pela companhia;
- Deve haver uma política formal de segurança da informação que aborde diretrizes de proteção de dados, classificação da informação, controle de acessos e gestão de incidentes. Essa política deve ser revisada periodicamente e disseminada para todos os colaboradores envolvidos na prestação de serviços;
- Os terceiros devem garantir que seus colaboradores estejam continuamente treinados e conscientizados sobre segurança da informação, participando de programas educacionais e campanhas de conscientização para reduzir riscos relacionados a ameaças internas e externas.

8.2 Proteção de Dados

- O Terceiro deve assegurar que todos os dados pessoais, sensíveis ou corporativos tratados estejam em conformidade com a LGPD, GDPR e demais regulamentações aplicáveis. Isso inclui a implementação de medidas técnicas como criptografia, pseudonimização e controle de acesso baseado em roles (RBAC);
- Dados considerados críticos (ex.: informações de passageiros, estratégias comerciais) devem ser armazenados exclusivamente em ambientes seguros, com restrição de acesso físico e lógico. A retenção de dados além do período necessário está estritamente proibida, salvo autorização formal da Companhia;
- É vedado ao Terceiro compartilhar, copiar ou transferir dados da Companhia para terceiros não autorizados, mesmo que parcialmente. Qualquer exceção requer aprovação prévia por escrito pela área jurídica e de segurança da informação da Companhia.

8.3 Gestão de Riscos

- O terceiro deve realizar avaliações periódicas de riscos de segurança da informação em seus processos e sistemas, identificando, analisando e tratando riscos potenciais que possam impactar a segurança das informações da companhia;
- Riscos identificados que possam comprometer a segurança ou a continuidade das operações devem ser comunicados em até 48 horas para a companhia e tratados conforme diretrizes estabelecidas, com a implementação de medidas corretivas e preventivas apropriadas.

8.4 Gerenciamento de Contas e Acessos

O Terceiro deve possuir um processo formal de Gerenciamento de Acessos que considere:

- Não permitir o uso de contas compartilhadas ou usuários genéricos, tal qual mantém controles relacionados a login, como forçar alteração no primeiro acesso, bloquear o usuário com determinadas tentativas inválidas, exigir padrão de senha

complexa;

- Concessão, alteração e revogação de acessos, principalmente àqueles com ações privilegiadas;
- Estabelecer métodos para controle de acesso físico e lógico de visitantes;
- Possuir controles de VPN e afins para acesso remoto dos colaboradores em período de trabalho remoto;
- O terceiro deve adotar princípios de menor privilégio e segregação de funções no gerenciamento de acessos, garantindo que cada usuário possua apenas as permissões estritamente necessárias para a execução de suas funções;
- Contas de acesso devem ser controladas e monitoradas rigorosamente, garantindo rastreabilidade, segurança e prevenindo acessos não autorizados. Procedimentos de revisão periódica de acessos devem ser implementados para garantir a conformidade com as políticas da companhia.

8.5 Gestão de Ativos

- Todos os ativos de informação utilizados devem ser inventariados, protegidos e gerenciados de forma adequada para evitar acessos não autorizados, roubo ou perda de dados sensíveis;
- Equipamentos e sistemas utilizados para tratamento de dados da companhia devem possuir controles de segurança como criptografia, proteção contra malware e mecanismos de controle de acesso.

8.6 Segurança nas Operações

- Devem ser aplicados controles de segurança adequados para garantir a integridade, disponibilidade e confiabilidade dos serviços prestados, prevenindo falhas e ataques cibernéticos;
- Processos de backup e recuperação de dados devem ser implementados e testados regularmente para garantir a continuidade dos serviços em caso de incidentes;
- Possuir um processo de execução de backups, o qual seja realizado

periodicamente nos ativos que armazenam informações da Companhia, de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes.

8.7 Gerenciamento de Logs e Incidentes

- Assegurar que dispõe do mais alto nível de capacidade no provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- Informar e dar acesso à Companhia, quando solicitado, sobre os recursos de gestão adequados ao monitoramento dos serviços contratados;
- Possuir equipes e ferramentas dedicadas para o monitoramento de capacidade e disponibilidade dos seus ativos, correlacionando alertas e gerando tickets de incidentes de forma automatizada;
- Possuir um processo estruturado de Resposta a Incidentes, contemplando a categorização dos incidentes e *runbooks* para tratamento e resolução de incidentes já conhecidos;
- Manter a Companhia permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor;
- Incidentes de segurança devem ser reportados em até **24 horas** via e-mail (**csirt@voegol.com.br**), seguindo o modelo estipulado em contrato. O **Terceiro** é responsável por conduzir análises root cause e apresentar relatório de lições aprendidas em até **10 dias** após a resolução. Ainda, incidentes devem ser tratados conforme procedimentos estabelecidos, garantindo a mitigação de impactos e a implementação de medidas corretivas eficazes.

8.8 Gerenciamento de Vulnerabilidades

- O Terceiro deve prevenir, detectar e reduzir vulnerabilidades propensas a se materializarem como incidentes relacionados com o ambiente cibernético, evidenciando os seus melhores esforços usando de procedimentos e controles, que

abranjam, no mínimo, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de dados, a realização periódica de testes e varreduras para detecção de vulnerabilidade, a aplicação de patches de segurança, a aplicação de *hardening* em seus servidores e estações de trabalho, a proteção contra softwares maliciosos e bloqueio de softwares não homologados, o estabelecimento de mecanismos de rastreabilidade e de segmentação da rede de computadores, a manutenção de cópias de segurança dos dados e das informações;

- Testes de invasão (*pentests*) devem ser conduzidos anualmente em sistemas/serviços contratados pela Companhia. Relatórios detalhados devem ser compartilhados, incluindo evidências de exploração e recomendações de correção, assim como sua própria mitigação.

8.9 Desenvolvimento Seguro

- Caso o **Terceiro** desenvolva softwares e estes sejam fornecidos à Companhia, deve desenvolver sistemas levando em consideração os padrões de segurança e privacidade (no âmbito da Lei Geral de Proteção de Dados) aceitos pelo mercado (*Privacy and Security by Design*) e OWASP Top 10 e integrar práticas de *Secure Software Development Lifecycle* (S-SDLC), incluindo, mas não se limitando à:
    - Revisões de código estático e dinâmico.
    - Testes de segurança automatizados em pipelines CI/CD.
    - Validação de bibliotecas de terceiros contra o banco de dados de vulnerabilidades conhecidas (ex.: NVD).

8.10 Segurança nas Comunicações

- Todas as comunicações eletrônicas envolvendo dados da Companhia devem utilizar protocolos de criptografia robustos. A utilização de redes públicas (Wi-Fi não seguras) para transmissão de dados sensíveis é expressamente proibida;
- Soluções de e-mails devem ser protegidos por soluções de segurança e de transferência segura;

- Informar e dar acesso à Companhia, quando solicitado, sobre as medidas de segurança para a transmissão e armazenamento dos dados e informações, bem como o seu descarte, utilizando procedimentos seguros de exclusão (mídia e papel).

8.11 Segurança Física

- O terceiro deve garantir que as instalações onde os serviços são prestados possuam controles físicos adequados, como controle de acesso, câmeras de monitoramento e segurança patrimonial.

8.12 Continuidade de Negócios e Gestão de Crise

- Definir um programa de continuidade de negócios, para assegurar que possíveis incidentes não afetem os serviços prestados à GOL, contemplando especialmente o plano de recuperação de desastres, testando regularmente os controles de asseguração a fim de se verificar a quão preparada a empresa está para casos reais;
- Cópias do plano devem ser disponibilizadas para revisão pela Companhia;
- Em situações de crise (ex.: ataques *ransomware*, desastres naturais), o Terceiro deve ativar imediatamente uma equipe de resposta a crises, composta por representantes técnicos, jurídicos e de comunicação, para coordenar ações com a Companhia.

8.13 Treinamento e Conscientização

- O Terceiro é integralmente responsável por assegurar que todos os seus funcionários, diretores, acionistas e intermediários recebam treinamentos adequados acerca de um programa anual de treinamento e conscientização em Segurança da Informação e Privacidade de Dados para todos os colaboradores;
- Contemplar em seu programa de treinamento e conscientização de segurança e privacidade de dados, campanhas como *phishing*, orientação sobre engenharia social, palestras externas, boletins informativos de SI e Privacidade de Dados etc;

- Os terceiros que acessarem ou processarem dados no ambiente da Companhia, devem ter ciência desta Política e do que diz respeito a treinamento de segurança da informação provido pela Companhia;
- Caso colaboradores do Terceiro sejam alocados para atividades junto à Companhia, por meio de body shop ou alocação de recursos — isto é, profissionais temporariamente alocados para atuar diretamente na equipe da GOL sem vínculo empregatício com esta —, deverão participar dos treinamentos internos de conscientização em segurança da informação e cibernética indicados pela área de Segurança Cibernética da GOL.

9 Controle de Registros

N/A.

10 Controle de Revisões

Revisão	Data	Páginas afetadas	Descrição da Modificação
00	22/01/2024	Todas	Emissão inicial.
01	12/06/2025	Todas	Revisão total.

11 Anexos

N/A.