PUBLIC DOCUMENT

POLÍTICA DE SEGURANÇA CIBERNÉTICA, DA INFORMAÇÃO E PRIVACIDADE

Italtel Brasil

Data	22/04/2025
Classe de Confidencialidade	Documento Público
Referências	ANATEL Resolução nº 740, de 21 de dezembro de 2020.

Indice

1 OBJETIVO 3
2 PÚBLICO-ALVO 3
3 DOS PRINCÍPIOS DE SEGURANÇA 3
4 PAPEIS E RESPONSABILIDADES 4
5 DIRETRIZES DE SEGURANÇA CIBERNÉTICA 6
6 PROCEDIMENTOS E CONTROLE 7
7 MEDIDAS DISCIPLINARES 8
8 REVISÕES 8

1 OBJETIVO

Este documento estabelece os princípios, conceitos, valores e referências a serem adotados visando assegurar a confidencialidade, a integridade e a disponibilidade das informações e dos dados da ITALTEL Brasil ou por ela controlados e dos sistemas de informação por ela utilizados. Permitindo à ITALTEL Brasil prevenir, detectar, reduzir e tratar as vulnerabilidades a incidentes relacionados à segurança da informação e ao ambiente cibernético. Proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2 PÚBLICO-ALVO

Este documento é dirigido a todas e quaisquer pessoas que tenham acesso as informações e dados da ITALTEL Brasil ou por ela controlados e aos sistemas por ela utilizados, como e não se limitando aos sócios, administradores, colaboradores, empregados ou não, menores aprendizes, estagiários, correspondentes, prestadores de serviços e terceiros.

3 DOS PRINCÍPIOS DE SEGURANÇA

As ações da ITALTEL Brasil regem-se pelos seguintes princípios:

i. Confidencialidade: limitação do acesso à informação, sendo permitido o acesso somente às pessoas autorizadas e em circunstâncias que se apresentem efetivamente necessário o acesso, protegendo informações que devem ser acessíveis apenas por um determinado grupo de usuários contra acessos não autorizados.
ii. Disponibilidade: garantia de acesso das pessoas devidamente autorizadas à informação sempre que o acesso for necessário, prevenindo interrupções das operações da ITALTEL Brasil por meio de um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança.
iii. Integridade: garantia da veracidade, fidelidade e integridade da informação e dos métodos de seu processamento e eventual tratamento da informação, pois esta não deve ser alterada enquanto está sendo transferida ou armazenada, impedindo que a informação fique exposta ao manuseio por uma pessoa não autorizada e impedindo alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.

4 PAPEIS E RESPONSABILIDADES

As responsabilidades atribuídas são distribuídas da seguinte forma:

4.1 Política de segurança cibernética e da informação, plano de ação e de resposta a incidentes: Política de Segurança Cibernética, da Informação e Privacidade, como direcionado pela norma ISO ABNT 27001:2022, é de responsabilidade da Alta Direção, sendo representado CISO. Em relação ao Plano de Ação e de Resposta a Incidentes e a melhoria contínua dos procedimentos técnicos relacionados ao tema são de responsabilidade do SOC interno da ITALTEL Brasil apoiar o CISO.

4.2 Registro, análise da causa e do impacto e controle dos efeitos de incidentes relevantes: O registro, a análise da causa e do impacto e o controle dos efeitos de incidentes relevantes são de responsabilidade do Comitê de Cibersegurança.

4.3 Realização dos testes e varreduras periódicos para detecção de vulnerabilidade: A realização dos testes e varreduras periódicos para detecção de vulnerabilidades são responsabilidades da área de Red Team e SOC interno da ITALTEL Brasil.

4.4 Manutenção de cópias de segurança dos dados e das informações: A execução dos backups, independentemente da plataforma computacional, bem como o descarte de mídias magnéticas oriundas do processo de backup, quando aplicável, são responsabilidades da Área de Tecnologia da Informação.

4.5 Documentação da verificação de capacidade do potencial prestador de serviço, das práticas de governança corporativa e da avaliação da relevância do serviço a ser contratado: A atividade de documentação das informações referente à verificação de capacidade do potencial prestador de serviço, das práticas de governança corporativa e referente à avaliação da relevância do serviço a ser contratado, são responsabilidades da Área de Compliance com auxílio das Áreas de Tecnologia da informação e a Área de Segurança da informação.

4.6 **Elaboração do relatório anual sobre a implementação do plano de ação e de resposta a incidentes:** A elaboração do relatório anual sobre a implementação do plano de ação e de resposta a incidentes, é responsabilidades do CISO.

4.7 **Comunicação de incidentes de segurança que impactem na privacidade à autoridade nacional de proteção de dados:** Em atenção ao Art. 48 da Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais - LGPD), será responsabilidade do Encarregado de Proteção de Dados (DPO), após ser cientificada pela Área de Tecnologia da Informação, comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

4.8 **Comunicação de contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem:** Será responsabilidade da Área de Segurança da informação, após ser comunicada pela Área de Tecnologia da Informação, a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem.

4.9 **Encarregado pelo tratamento de dados pessoais:** Em atenção aos artigos. 5º, inciso VIII; 23, inciso II; e 41, caput e parágrafos, todos da Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais - LGPD), na qualidade de “Encarregado pelo Tratamento de Dados Pessoais”, esta pessoa indicada pelo controlador irá atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

5 DIRETRIZES DE SEGURANÇA CIBERNÉTICA

5.1 **Das diretrizes para tratamento da Informação:** A informação deve receber proteção adequada em observância aos princípios e diretrizes da Segurança Cibernética, da Informação e Privacidade da ITALTEL Brasil em todo o seu ciclo de vida, que compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.

5.2 **Das diretrizes para classificação de dados e das informações:** As informações e os dados sob responsabilidade da ITALTEL Brasil serão classificados, conforme descrito no plano de ação, para adequação das estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética.

5.3 **Das diretrizes para a elaboração de cenários de incidentes considerados nos testes de continuidade de negócios:** Deverão ser elaborados, no âmbito dos testes de continuidade de negócios, cenários de incidentes que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados pela ITALTEL Brasil, que tenham ou possam ter a capacidade de causar disrupções nos processos de negócios da companhia.

5.4 **Das diretrizes para a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços**: Na elaboração de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços ou parceiras, considerando as características do serviço a ser prestado e níveis de complexidade, abrangência e precisão, deverão ser analisados cenários de incidentes que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados.

5.5 Das diretrizes para definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes: Os parâmetros a serem utilizados na avaliação da relevância dos incidentes deverão considerar a frequência e o impacto dos cenários de incidentes que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados, que tenham ou possam ter a capacidade de causar interrupção nos processos de negócios da ITALTEL Brasil..

5.6 Das diretrizes para definição dos parâmetros a serem utilizados na retenção e descarte de dados pessoais: A informação deve receber proteção adequada em observância aos princípios e diretrizes da Segurança Cibernética, da Informação e Privacidade da ITALTEL Brasil em todo o seu ciclo de vida, incluindo o Descarte adequado para informações digitais e/ou físicas.

6 PROCEDIMENTOS E CONTROLE

Para reduzir a vulnerabilidade da ITALTEL Brasil a incidentes e atender aos demais objetivos de segurança cibernética, da informação e privacidade, a organização, inclusive, na adoção de novas tecnologias, adotará as seguintes políticas específicas por tem:

- Política de Resposta a Incidentes;
- Política de Gestão de Vulnerabilidades;
- Política de Backup;
- Política de Gestão de Fornecedores;
- Política de Privacidade;
- Política de Classificação de Dados e Informação;
- Política de Gestão de Acessos;
- Política de Criptografia;
- Política de Uso Aceitável de Recursos;
- Política de Continuidade de Negócios;
- Política de Desenvolvimento de Software Seguro;
- Política de Retenção e Descarte de Dados

O documento relativo à Política de Segurança Cibernética, da Informação e Privacidade deve estar sempre disponível, assim como as demais as documentações: planos de ação, políticas específicas por tema, relatórios anuais, registros de acompanhamento e de controle da implementação da efetividade das políticas.

7 MEDIDAS DISCIPLINARES

As violações a esta política estão sujeitas às sanções disciplinares previstas, nas normas internas da ITALTEL Brasil e na legislação vigente no Brasil e nos países onde a empresa estiver localizada.

8 REVISÕES

Esta política será documentada e revisada a cada dois anos, ou em período referente após mudança significativa de processos, pessoas ou tecnologias que impactem no Sistema de Gestão de Segurança da Informação. As políticas advindas desta, deverão seguir a mesma periodicidade mencionada.