

POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO E SEGURANÇA DA INFORMAÇÃO

EMPREGADOR: J R Serviços e Consultoria Ltda – Telétrica

CNPJ: 04.452.896/0001-09

A informação é um dos ativos mais importantes da **Telétrica**. Esta Política estabelece as diretrizes para utilização adequada dos recursos tecnológicos e as responsabilidades quanto à segurança da informação, preservando a confidencialidade, a integridade e a disponibilidade dos dados. Constitui a política guarda-chuva do sistema de segurança da informação da **Telétrica**, sendo detalhada por políticas e procedimentos específicos relacionados no item 12.

1. ABRANGÊNCIA E PRINCÍPIOS

Aplica-se a sócios, administradores, gestores, colaboradores, estagiários, aprendizes, prestadores de serviços e terceiros que utilizem recursos tecnológicos da **Telétrica**. Observa os princípios de confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, mínimo privilégio, segurança por padrão, privacidade desde a concepção (Privacy by Design) e gestão baseada em risco.

2. ORGANIZAÇÃO E RESPONSABILIDADES PELA SEGURANÇA DA INFORMAÇÃO

A segurança da informação é responsabilidade de todos, com a seguinte estrutura de governança, proporcional ao porte da **Telétrica**:

- Diretoria: responsável pela aprovação das políticas, provisão de recursos, supervisão dos controles e decisão sobre tratamento e aceitação de riscos.
- Responsável pela Segurança da Informação e TI: encarregado de implementar, operar, monitorar e documentar os controles de segurança, tratar incidentes e conduzir as revisões periódicas.
- Encarregado pelo Tratamento de Dados Pessoais (DPO): responsável pelas atribuições da LGPD, conforme a Política de Privacidade (POL-LGPD-001). [Indicar o nome do Encarregado.]
- Usuários: responsáveis por cumprir as políticas, proteger suas credenciais e comunicar eventos suspeitos.

Segregação de funções: dada a dimensão da equipe, quando quem executa um controle não puder ser distinto de quem o supervisiona, a Diretoria exerce a função de revisão e aprovação, garantindo controle a quatro mãos sobre as atividades sensíveis (acessos, backups e incidentes).

3. UTILIZAÇÃO DOS RECURSOS E CONTROLE DE ACESSO

Os recursos tecnológicos (computadores, notebooks, tablets, celulares corporativos, sistemas, e-mail, redes, serviços em nuvem e aplicativos) destinam-se prioritariamente às atividades profissionais. As credenciais são pessoais e intransferíveis, sendo proibido compartilhar senhas, utilizar credenciais de terceiros, anotá-las em locais inseguros ou permitir acesso não autorizado. Os usuários deverão criar senhas seguras, alterá-las quando solicitado e comunicar suspeitas de comprometimento. A autenticação multifator (MFA) é obrigatória. As regras detalhadas constam da Política de Controle de Acesso (POL-TI-003) e do Procedimento de Gestão de Usuários e Acessos (PRO-TI-002).

4. E-MAIL, MENSAGENS, INTERNET E REDES SOCIAIS

O e-mail e os aplicativos de mensagens corporativos são ferramentas de trabalho e devem observar linguagem profissional, proteção de informações confidenciais e verificação de destinatários. É vedado enviar conteúdo ofensivo ou discriminatório, transmitir informações sigilosas sem autorização, acessar conteúdos ilícitos, utilizar redes sociais para ofender colegas, clientes ou parceiros, ou divulgar informações internas sem autorização.

5. EQUIPAMENTOS, DISPOSITIVOS E ARMAZENAMENTO

Os equipamentos permanecem de propriedade da **Telétrica** e devem ser conservados e utilizados adequadamente, com comunicação imediata de perdas, furtos ou danos. Os dispositivos são gerenciados e protegidos (ex.: criptografia de disco, bloqueio de tela e limpeza remota via Intune, quando aplicável). Os documentos corporativos deverão ser armazenados apenas em locais autorizados e cobertos por backup (servidores, sistemas internos e plataformas aprovadas), sendo vedado o armazenamento em dispositivos ou serviços não autorizados. As diretrizes de cópia e recuperação constam da Política de Backup e Recuperação (POL-TI-002).

6. DADOS PESSOAIS E PRIVACIDADE

Os dados pessoais somente poderão ser tratados para finalidades legítimas, conforme a LGPD e a Política de Privacidade e Proteção de Dados Pessoais (POL-LGPD-001), observados o princípio da minimização e o descarte seguro ao fim de sua finalidade (Política de Descarte Seguro, POL-TI-004).

7. UTILIZAÇÃO DE INTELIGÊNCIA ARTIFICIAL

As ferramentas de IA podem contribuir para a produtividade, observados critérios de segurança, confidencialidade e conformidade. É proibido inserir em ferramentas de IA públicas dados pessoais de colaboradores ou clientes, informações sigilosas, contratos, informações estratégicas e dados protegidos por confidencialidade. Todo conteúdo gerado por IA deverá ser analisado criticamente, permanecendo o usuário responsável pelas informações produzidas.

8. MONITORAMENTO E PRIVACIDADE

Os recursos tecnológicos corporativos poderão ser monitorados pela **Telétrica** para fins de segurança da informação, auditoria, investigação de incidentes, proteção patrimonial e cumprimento de obrigações legais. O monitoramento recai exclusivamente sobre as ferramentas e contas corporativas disponibilizadas pela empresa, das quais o usuário tem ciência prévia, não alcançando contas, dispositivos ou comunicações de caráter estritamente pessoal. O monitoramento observará a legislação aplicável, os princípios da LGPD e os direitos dos usuários.

9. SEGURANÇA CIBERNÉTICA E INCIDENTES

Todos os usuários devem contribuir para a prevenção de incidentes, comunicando imediatamente situações suspeitas (e-mails fraudulentos, tentativas de golpe, solicitações suspeitas de dados, links desconhecidos e programas não autorizados). A rapidez na comunicação é fundamental para reduzir impactos. O tratamento de incidentes segue o Procedimento de Resposta a Incidentes de Segurança da Informação (PRO-TI-001), incluindo as obrigações de notificação previstas na LGPD e nos contratos com clientes.

10. GESTÃO DE RISCOS

A **Telétrica** adota a gestão baseada em risco: os riscos de segurança da informação e privacidade são identificados, avaliados, tratados e monitorados de forma proporcional, conforme a Política de Gestão de Riscos (POL-TI-005) e a Matriz de Riscos correspondente.

11. DESLIGAMENTO OU ALTERAÇÃO DE FUNÇÃO

No encerramento do vínculo ou alteração de função, o usuário deverá devolver equipamentos, ter acessos encerrados ou ajustados, restituir documentos corporativos e preservar a confidencialidade das informações obtidas durante o vínculo, conforme o Procedimento de Gestão de Usuários e Acessos (PRO-TI-002).

12. DOCUMENTOS RELACIONADOS

Esta Política é complementada e detalhada pelos seguintes documentos:

Código	Documento
POL-TI-002	Política de Backup e Recuperação de Dados
POL-TI-003	Política de Controle de Acesso
POL-TI-004	Política de Descarte Seguro de Dados e Mídias
POL-TI-005	Política de Gestão de Riscos
PRO-TI-001	Procedimento de Resposta a Incidentes de Segurança da Informação
PRO-TI-002	Procedimento de Gestão de Usuários e Acessos
POL-LGPD-001	Política de Privacidade e Proteção de Dados Pessoais
POL-RH-003	Política de Consequências e Medidas Disciplinares

13. MEDIDAS DISCIPLINARES, REVISÃO, APROVAÇÃO E VIGÊNCIA

O descumprimento poderá resultar nas medidas disciplinares cabíveis (POL-RH-003) e em responsabilizações civis, administrativas ou criminais. Esta Política será revisada ao menos anualmente ou quando houver mudança relevante. Entra em vigor na data de sua aprovação pela Diretoria, permanecendo válida até sua revisão formal.

Aprovado por:

Documento assinado digitalmente
 VICTOR VILAR RAPOZO
Data: 05/09/2026 14:43:51-0300
Verifique em <https://validar.iti.gov.br>

Diretor