Mobili

Mantenha-se Conectado

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

COMITÊ DE SEGURANÇA DA INFORMAÇÃO

MOBILI BRASIL SERVICOS DE TELECOMUNICACOES

| | |
|---|---|
| Versão | 2.0 |
| Data da Versão | 15/07/2026 |
| Responsável | Fabrício Alves Pereira |
| Classificação | Publico |
| Aprovado por | Comitê de Segurança da Informação |

## Sumário

# 1. Finalidade, escopo e usuários

O objetivo desta Política de alto nível é definir a finalidade, a direção, os princípios e as regras básicas de gestão da segurança da informação.

Esta política aplica-se a todo o Sistema de Gestão da Segurança da Informação (SGSI), como definido no documento de escopo do SGSI.

Este documento, assim como toda a documentação referente ao Sistema de Gestão, é de propriedade da Mobili, divulgados e controlados pela área de tecnologia da informação, sendo proibida a reprodução indevida ou divulgação destes documentos sem consentimento prévio.

A Segurança da Informação visa a preservação da confidencialidade, integridade e disponibilidade da informação. Adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade. A segurança compreende, assim, a proteção das informações em relação aos diversos tipos de ameaças para: · garantir a continuidade do negócio; · minimizar o risco ao negócio; · maximizar o retorno sobre os investimentos e as oportunidades de negócio.

Os usuários deste documento são todos os colaboradores, contratados, prestadores de serviços da Mobili, assim como as partes externas relevantes.

# 2. Referências

- Norma ISO/IEC 27001, em sua versão atual
- Lei nº13.709/2018 - Lei Geral de Proteção de Dados (“LGPD”).
- Lista de requisitos legais, regulamentares, contratuais e outros.

# 3. Gerenciando a segurança da informação

## 3.1. Objetivos e medição

Os objetivos do Sistema de Gestão foram estabelecidos pelo Comitê de Segurança da Informação com o objetivo de buscar a melhoria contínua dos processos e serviços, preservando a segurança da informação das partes interessadas. Tais objetivos foram estabelecidos de forma a garantir:

- **Manter a Certificação da Norma ISO/IEC 27001 e Evoluir a Conformidade:** Assegurar a manutenção contínua do selo ISO/IEC 27001 por meio de auditorias internas regulares, análise crítica do Comitê e tratamento eficaz de melhorias, consolidando o compromisso permanente da organização com as melhores práticas globais de segurança.
- **Consolidar a Competência e a Alta Performance das Equipes de TI e SI:** Promover a reciclagem técnica contínua e o desenvolvimento avançado das equipes do NOC e do SOC, garantindo que os analistas operem com alta eficácia na correlação de eventos, resposta a incidentes complexos e gestão de infraestrutura de conectividade.
- **Alavancar a Credibilidade e o Posicionamento de Mercado:** Utilizar a maturidade do SGSI e o cumprimento das regulamentações (como a LGPD) como diferencial competitivo, fortalecendo a reputação da MOBILI frente a clientes estratégicos, parceiros institucionais e reguladores como uma operadora resiliente e segura.
- **Otimizar e Auditar os Controles de Proteção de Acesso a Sistemas**: Refinar continuamente as barreiras lógicas e os perímetros de segurança da infraestrutura corporativa, garantindo a aplicação rigorosa do princípio do menor privilégio e realizando revisões trimestrais para impedir acessos obsoletos ou não autorizados.

- **Garantir a Resiliência da Autenticação Multifator (MFA) Corporativa:** Manter a obrigatoriedade e auditar a cobertura de 100% do uso de Autenticação Multifator (MFA) para todos os acessos lógicos a sistemas, servidores e consoles centrais da organização, eliminando brechas de credenciais comprometidas.
- **Sustentar a Cultura de Segurança da Informação e Privacidade:** Evoluir os programas de conscientização e treinamentos periódicos, transformando o conhecimento inicial em uma cultura organizacional viva, onde todos os colaboradores compreendam e apliquem ativamente suas responsabilidades diárias na proteção de dados e ativos.

- Para cada objetivo é associado um ou mais indicadores cujas metas são atribuídas e revisadas em períodos pré defindos pela direção em reunião de análise crítica, conforme descrito no documento "Objetivos monitoramento medição e análise".

- Os objetivos dos controles de segurança ou grupos de controles são definidos pela alta direção da Mobili e aprovados pelo Comitê de Segurança da Informação na Declaração de aplicabilidade.

- A Alta Direção assegura que esta Política e os Objetivos de Segurança da Informação sejam revisados periodicamente, ou sempre que ocorrerem mudanças relevantes no contexto organizacional, na direção estratégica, nos requisitos das partes interessadas ou no escopo do Sistema de Gestão da Segurança da Informação.

- A Mobili irá mensurar o atendimento de todos os objetivos. O responsável pela área de tecnologia da informação em conjunto com os responsáveis pelas áreas de SOC e NOC, são os responsáveis por definir o método para a medição da realização dos objetivos. A medição será executada ao menos uma vez por ano e o responsável pela área de projetos que irá analisar a avaliar os resultados da medição e reportá-los para a alta direção da Mobili como materiais de entrada para a análise crítica.

- O responsável pela área de Projeto é responsável por registrar os detalhes sobre os métodos de medição, periodicidades e resultados no relatório de medição.

### 3.2. Requisitos de segurança da informação

- Esta Política e todo o SGSI deve estar em conformidade com os requisitos legais e regulamentares levantes à organização, bem como com as obrigações contratuais, e deverá ser comunicada a todos os colaboradores, clientes, prestadores de serviços a fim de que a política seja cumprida dentro e fora da empresa.

- O não cumprimento dos requisitos previstos neste documento acarretará violação às regras internas da Mobili, e sujeitará o usuário às medidas administrativas e legais cabíveis.

### 3.3. Controles da segurança da informação

- Os processos para selecionar os controles (salvaguardas) estão definidos na Metodologia de avaliação e tratamento de riscos.

- Os controles selecionados e seu status de implementação estão listados na Declaração de aplicabilidade.

### 3.4. Controles e Ativos Críticos de TI

- **Diretriz de Infraestrutura e Conectividade Crítica:** Ficam formalmente classificados como **Ativos Críticos de Informação e Operação** da Mobili todos os dispositivos de infraestrutura central de rede (roteadores, switches de distribuição, firewalls de borda) e os elementos de recepção e transmissão de dados (antenas, modems e gateways das soluções operacionais).

- O monitoramento destes ativos deve ser centralizado e ininterrupto (24x7) pela equipe do NOC (Network Operations Center), utilizando a ferramenta Zabbix para a coleta de métricas de integridade elétrica, temperatura, latência, consumo de banda e perda de pacotes, disparando alertas proativos para mitigação imediata de incidentes.

## 4. Responsabilidades

### Comitê de Segurança da Informação

- Aprovar formalmente a Política de Segurança da Informação e garantir sua divulgação e compreensão em todos os níveis da organização.
- Alocar os recursos financeiros, humanos e tecnológicos adequados para a implementação, manutenção e aprimoramento contínuo das medidas de segurança da informação.
- Definir os objetivos estratégicos de segurança da informação, alinhados aos objetivos de negócio da Mobili.
- As responsabilidades operacionais específicas de tratamento de rede e segurança estão detalhadas na Matriz de Responsabilidades (RACI) do SGSI.
- Garantir que a empresa esteja em conformidade com todas as leis, regulamentações e requisitos contratuais relacionados à segurança da informação.

### Tecnologia da Informação

- Implementar, configurar e manter os controles de segurança técnica, incluindo firewalls, sistemas de detecção e prevenção de intrusão (IDS/IPS), antivírus, sistemas de backup e recuperação de desastres, gestão de acessos e criptografia.
- Estabelecer e operar um processo de gestão de incidentes de segurança, incluindo detecção, análise, contenção, erradicação, recuperação e pós-incidente.
- Gerenciar o ciclo de vida das contas de usuário e permissões de acesso a sistemas e dados, garantindo o princípio do menor privilégio.
- Monitorar continuamente os sistemas e a rede em busca de atividades suspeitas e realizar auditorias regulares para garantir a conformidade com a PSI.
- Colaborar com a área de administração e projetos na criação e execução de programas de conscientização e treinamento em segurança da informação para todos os colaboradores.
- Publicar e manter disponível a Política de Segurança da Informação (PSI) no site oficial da organização (**www.mobili.net.br**), garantindo a transparência e a fácil acessibilidade das diretrizes de segurança para colaboradores, parceiros e clientes.
- Assegurar que os fornecedores de serviços e produtos de TI cumpram os requisitos de segurança da informação da empresa.

### Colaboradores

- Ler, compreender e cumprir todas as políticas, procedimentos e diretrizes de segurança da informação estabelecidas pela empresa.
- Proteger as informações e os ativos de TI sob sua responsabilidade contra acesso não autorizado, modificação, destruição ou divulgação.
- Utilizar os recursos de tecnologia da informação da empresa (computadores, sistemas, redes, e-mail, internet) de forma ética, responsável e de acordo com as políticas.
- Proteger senhas e outras credenciais de acesso, não as compartilhando com terceiros e alterando-as regularmente conforme as políticas.
- Reportar assim que identificar, quaisquer incidentes de segurança da informação, através do e-mail:

suporte@mobili.net.br, (ex: e-mails de phishing, perda/roubo de dispositivos, atividades suspeitas).

- Tratar informações de acordo com seu nível de confidencialidade, evitando sua divulgação indevida, seja verbalmente, por escrito ou eletronicamente.
- Seguir as políticas da empresa relacionadas ao uso de dispositivos pessoais (BYOD - Bring Your Own Device) para fins de trabalho, garantindo a segurança dos dados corporativos.

**Encarregado de Proteção de Dados (DPO)**

Responsável por atuar como canal de comunicação oficial com titulares e órgãos reguladores, além de orientar a organização sobre conformidade com a LGPD.

- **Tecnologia da Informação e Comunicação (TIC):** Responsável por garantir a sustentação tecnológica, segurança, licenciamento e monitoramento preventivo de disponibilidade de todos os canais de comunicação institucionais do SGSI

## 5. Suporte para a implementação do SGSI

A alta administração da Mobili declara que a implementação do SGSI e seu contínuo aprimoramento serão suportadas pelos recursos apropriados para alcançar todos os objetivos definidos nesta Política, assim como atender todos os requisitos identificados.

### 5.1. Gestão de Vulnerabilidades Técnicas e Prazos de SLA

O processo de Gestão de Vulnerabilidades Técnicas tem por objetivo identificar, avaliar e mitigar riscos preventivamente na infraestrutura de TI, nos ativos de nuvem e nos sistemas de inteligência de rede monitorados pelo SOC e NOC.

### 5.2. Ciclo de Emissão do Relatório de Vulnerabilidade

A identificação e o registro de vulnerabilidades devem ocorrer de forma contínua e sistemática, obedecendo às seguintes janelas de execução:

- **Relatório Mensal de Vulnerabilidades Lógicas:** Consolidação mensal de análises de superfícies de ataque, relatórios de *scans* automatizados no ambiente AWS, e logs consolidados das ferramentas de proteção (EDR, XDR, WAF, API Security e SIEM). Este relatório serve como insumo direto para as reuniões do Comitê de Segurança da Informação.

- **Relatório de Desempenho e Disponibilidade:** Emissão mensal de relatórios gerados via ferramentas de monitoramento de performance (Zabbix/Grafana), correlacionando gargalos de infraestrutura que possam gerar vulnerabilidades de negação de serviço (DoS/DDoS).

- **Relatório Anual de Teste de Intrusão (Pentest):** Realização anual de testes de intrusão por auditoria externa independente em todo o perímetro lógico e aplicações críticas da Mobili Brasil.

### 5.3. Matriz de Criticidade e Prazos de Remediação (SLA)

Uma vez gerado o Relatório de Vulnerabilidade, os planos de ação para a aplicação de correções (*patches*), atualizações ou mitigações temporárias deverão seguir rigorosamente os prazos de Acordo de Nível de Serviço (SLA) abaixo, contados a partir da data de classificação do risco:

| Criticidade do Risco | Descrição Técnico-Operacional | Prazo Máximo para Correção | Responsável pela Validação |
|---|---|---|---|
| **Crítica (Critical)** | Vulnerabilidades com exploração ativa no mercado, sem necessidade de autenticação prévia e com alto impacto de vazamento de dados ou indisponibilidade sistêmica. | **Até 48 horas** | Responsável pelo SOC / TI |
| **Alta (High)** | Falhas estruturais que permitem elevação de privilégios ou o comprometimento direto de serviços importantes de rede e nuvem. | **Até 15 dias** | Responsável pelo SOC / NOC |
| **Média (Medium)** | Desvios de configuração, políticas frágeis ou softwares desatualizados que exigem condições complexas ou específicas para exploração. | **Até 30 dias** | Responsável pelo TI |
| **Baixa (Low)** | Informações expostas em cabeçalhos públicos ou vulnerabilidades menores de baixo impacto reputacional e operacional. | **Até 90 dias** *(ou aceitação formal)* | Comitê de Segurança da Informação |

| Tipo de Relatório | Frequência | Escopo / Ferramentas Envolvidas | Objetivo no SGSI |
|---|---|---|---|
| Relatório de Vulnerabilidades Lógicas | Mensal | Análise de superfícies de ataque, scans na AWS e logs de proteção (EDR, XDR, WAF, API Security e SIEM). | Servir como insumo direto para as reuniões e deliberações do Comitê de Segurança da Informação. |
| Relatório de Desempenho e Disponibilidade | Mensal | Métricas de performance e capacidade geradas via plataformas de monitoramento (Zabbix e Grafana). | Prevenir vulnerabilidades de negação de serviço (DoS/DDoS) e mitigar gargalos operacionais de infraestrutura. |
| Relatório de Teste de Intrusão | Anual | Testes de invasão controlados e executados por auditoria externa | Validar a eficácia real |

| | | | |
|---|---|---|---|
| (Pentest) | | independente. | dos perímetros lógicos e das aplicações críticas da Mobili Brasil. |

## 6. Validade e gestão de documentos

Este documento passa a ser válido a partir da data de aprovação do Comitê de Segurança da Informação.

O proprietário do documento é o responsável pela área de Tecnologia da Informação, que deve verificar e, se necessário, atualizar o documento pelo menos uma vez por ano.

Ao avaliar a eficácia e a adequação deste documento, os seguintes critérios devem ser considerados:

- quantidade de incidentes relacionados ao acesso não autorizado às informações
- quantidade de ativos de informações classificados com o nível de confidencialidade inadequado

### Penalidades e Consequências

O não cumprimento das diretrizes desta política poderá resultar em ações disciplinares, que podem incluir advertências, ou até rescisão contratual, dependendo da gravidade da infração. Em caso de incidentes de segurança, podem ser tomadas medidas corretivas adicionais.

### Treinamento e Conscientização

- Sensibilização: Todos os colaboradores devem ser devidamente informados e sensibilizados quanto às políticas de segurança da informação da organização, compreendendo sua importância para a proteção dos ativos e a continuidade do negócio.
- Conscientização sobre Segurança: A Mobili deve promover treinamentos periódicos com foco nas melhores práticas de segurança da informação, visando prevenir incidentes, reforçar comportamentos seguros e assegurar que cada colaborador conheça suas responsabilidades individuais no tratamento adequado das informações.

## 7. Histórico de alterações

| Data | Versão | Criado por | Descrição da alteração |
|---|---|---|---|
| 21/05/2025 | 0.1 | Fabrício Alves Pereira | Versão Inicial do documento |
| 15/12/2025 | 1.0 | Fabrício Alves Pereira | **Publicação Oficial da PSI.** Consolidação das diretrizes de segurança de alto nível, inclusão das responsabilidades do Comitê, TI e colaboradores, e incorporação das diretrizes de monitoramento 24x7 para ativos críticos de rede e conectividade (NOC/SOC).Atualização dos itens 3.1 5.1, 5.2 e 5.3 |
| 15/07/2026 | 2.0 | Fabrício Alves Pereira | Revisão da Política de Segurança da Informação para atendimento às ações |

| | | | |
|---|---|---|---|
| | | | corretivas decorrentes das NCs 03, 04, 06 e 07 da auditoria externa, contemplando a revisão dos Objetivos de Segurança da Informação, o alinhamento da política à direção estratégica da organização e ao escopo vigente do SGSI, bem como a atualização do processo de comunicação e disponibilização da política às partes interessadas. Alterações aprovadas pelo Comitê de Segurança da Informação (CSI) e registradas nos chamados do ITSM para fins de rastreabilidade e evidência de conformidade. |