POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO E IMPORTÂNCIA

A Política de Segurança da Informação da Investira Soluções tem como objetivo estabelecer diretrizes, responsabilidades e controles para proteger os ativos de informação da empresa contra ameaças internas e externas, garantindo a confidencialidade, integridade e disponibilidade das informações.

Esta Política é fundamental para:

- Manter a confiança de clientes, parceiros e colaboradores
- Garantir a continuidade dos negócios
- Cumprir requisitos legais e contratuais (LGPD, Marco Civil da Internet, contratos com clientes)
- Proteger a propriedade intelectual e vantagem competitiva
- Prevenir perdas financeiras e danos à reputação

2. ABRANGÊNCIA

Aplica-se a todos os ativos de informação da empresa, incluindo:

- Dados pessoais de clientes, colaboradores e terceiros
- Propriedade intelectual (código-fonte, algoritmos, patentes)
- Informações estratégicas e de negócio
- Infraestrutura tecnológica (hardware, software, rede)
- Documentos físicos e eletrônicos
- Aplicações e sistemas desenvolvidos e utilizados

E a todas as pessoas que acessam, utilizam ou administram estes ativos, independentemente do local (escritório, home office, viagens) ou dispositivo utilizado.

3. PRINCÍPIOS FUNDAMENTAIS

A segurança da informação na Investira é baseada na tríade CID:

3.1. Confidencialidade

A informação só deve ser acessível a pessoas, entidades ou sistemas autorizados. O acesso é concedido com base no princípio do "menor privilégio necessário".

3.2. Integridade

A informação deve ser mantida precisa, completa e protegida contra modificações não autorizadas durante todo o seu ciclo de vida.

3.3. Disponibilidade

A informação e os sistemas de suporte devem estar acessíveis e utilizáveis quando necessários pelos processos de negócio, dentro dos níveis de serviço acordados.

4. PAPÉIS E RESPONSABILIDADES

4.1. Diretoria Executiva

- Estabelecer e apoiar a cultura de segurança
- Alocar recursos adequados
- Aprovar esta Política e suas atualizações
- Definir a tolerância a riscos da organização

4.2. Comitê de Segurança da Informação

- Supervisionar a implementação da Política
- Analisar e aprovar o Plano de Tratamento de Riscos
- Avaliar incidentes de segurança significativos
- Recomendar melhorias e investimentos

4.3. Gestor de Segurança da Informação (CISO)

- Coordenar a implementação do SGSI
- Gerenciar o programa de conscientização
- Supervisionar a resposta a incidentes
- Reportar à Diretoria sobre o estado da segurança

4.4. Gestores de Área

- Implementar controles de segurança em suas áreas
- Garantir que colaboradores cumpram esta Política
- Reportar riscos e incidentes identificados
- Participar dos exercícios de continuidade de negócios

4.5. Todos os Colaboradores

- Conhecer e cumprir esta Política e procedimentos relacionados
- Proteger as credenciais de acesso (não compartilhar senhas)
- Reportar imediatamente incidentes ou suspeitas de segurança
- Participar dos treinamentos de segurança
- Utilizar os recursos da empresa apenas para fins autorizados

4.6. Equipe de TI e Segurança

- Implementar e manter controles técnicos
- Monitorar sistemas e redes em busca de ameaças
- Realizar testes de vulnerabilidade e penetração
- Gerenciar patches e atualizações de segurança
- Executar backups e testes de recuperação

5. CONTROLES DE SEGURANÇA

5.1. Controles de Acesso

- Autenticação multifator para sistemas críticos
- Senhas complexas e troca periódica
- Provisionamento e desprovisionamento automatizado
- Revisão periódica de privilégios de acesso
- Controle de acesso físico a data centers e salas de servidores

5.2. Segurança de Endpoints

Antivírus/antimalware atualizado em todos os dispositivos

- Criptografia de disco completo para laptops
- Política de uso aceitável para dispositivos corporativos
- Controle de dispositivos removíveis (USBs)
- Remote wipe para dispositivos móveis perdidos/roubados

5.3. Segurança de Rede

- Firewalls de próxima geração com inspeção profunda

- Segmentação de rede (VLANS)
- VPN segura para acesso remoto
- Monitoramento contínuo de tráfego (SIEM)
- Proteção DDoS

5.4. Segurança em Desenvolvimento (DevSecOps)

- Análise estática e dinâmica de código (SAST/DAST)
- Scans de vulnerabilidades em dependências
- Segurança em pipeline de CI/CD
- Treinamento específico para desenvolvedores em segurança
- Revisões de código com foco em segurança

5.5. Proteção de Dados

- Classificação de dados (público, interno, confidencial, restrito)
- Criptografia de dados em trânsito (TLS 1.3+) e em repouso
- Máscara/anominação de dados em ambientes não produtivos
- Política de retenção e destruição segura
- Prevenção de perda de dados (DLP)

5.6. Gestão de Vulnerabilidades

- Scan de vulnerabilidades trimestral
- Programa de bug bounty para produtos críticos
- Processo estruturado de patch management
- Priorização baseada em risco (CVSS)

5.7. Continuidade de Negócios e Recuperação de Desastres

- Plano de Continuidade de Negócios (BCP) documentado
- Planos de Recuperação de Desastres (DRP) por sistema crítico
- Backup automatizado e teste regular de restauração
- Sites de recovery (hot/warm) para sistemas essenciais
- Exercícios anuais de simulação

6. SEGURANÇA EM TELETRABALHO

- Conexão segura via VPN corporativa
- Wi-Fi doméstico com criptografia WPA3
- Dispositivos corporativos preferenciais (BYOD com políticas restritivas)
- Treinamento específico para segurança em home office
- Política de clean desk mesmo em ambiente doméstico

7. RESPOSTA A INCIDENTES

Processo estruturado em 6 fases:

7.1. Preparação

- Equipe de resposta a incidentes (CSIRT) treinada
- Plano de resposta documentado e testado
- Ferramentas de análise forense disponíveis

7.2. Identificação

- Monitoramento proativo
- Análise de alertas do SIEM
- Comunicação imediata ao CSIRT

7.3. Contenção

- Isolamento de sistemas afetados
- Coleta de evidências forenses
- Notificação inicial à Diretoria

7.4. Erradicação

- Remoção da causa raiz
- Aplicação de patches e correções
- Limpeza de sistemas comprometidos

7.5. Recuperação

- Restauração de sistemas a partir de backups limpos
- Monitoramento pós-incidente
- Retorno gradual às operações normais

7.6. Lições Aprendidas

- Análise pós-mortem detalhada
- Atualização de políticas e procedimentos
- Comunicação interna sobre aprendizados

8. CONFORMIDADE E AUDITORIA

- Auditoria interna anual de segurança
- Avaliação de conformidade com LGPD, ISO 27001 e outros requisitos
- Due diligence de segurança em aquisições e parcerias
- Manutenção de evidências para demonstrar conformidade

9. CONSCIENTIZAÇÃO E TREINAMENTO

- Treinamento obrigatório anual para todos os colaboradores
- Treinamentos específicos por função (desenvolvedores, administradores)
- Campanhas periódicas de phishing simulado
- Material de apoio em múltiplos formatos
- Programa de reconhecimento para comportamentos seguros

10. EXCEÇÕES E DISPOSIÇÕES FINAIS

Exceções a esta Política somente serão concedidas mediante aprovação formal por escrito do Comitê de Segurança, com justificativa técnica e plano de mitigação de riscos.

Esta Política será revisada anualmente ou quando mudanças significativas no ambiente de ameaças, negócio ou regulatório assim exigirem.