LINHAS GERAIS DA POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

1. OBJETIVO

A Política de Segurança Cibernética e da Informação (Política) do RAPPIBANK estabelece as diretrizes para minimizar os riscos de segurança da informação, seus ativos tecnológicos e/ou comunicações, garantindo que as obrigações legais e contratuais dos negócios sejam cumpridas, tendo como foco principal garantir a confidencialidade, integridade, disponibilidade e não repúdio dos dados e sistemas da Instituição ou por ela controlados, além de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados ao ambiente cibernético e proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2. APLICABILIDADE

Esta Política e demais políticas relacionadas devem ser cumpridas por toda e qualquer pessoa que tenha relacionamento com as atividades do RAPPIBANK (todos os colaboradores, parceiros, fornecedores de serviço etc.), abrangendo todas as informações e o ambiente computacional desta Instituição.

3. PRINCÍPIOS

Os princípios estão definidos na Política e devem ser respeitados por todos a quem a Política se aplica.

4. POLÍTICA

Esta Política está em conformidade com a legislação aplicável e normas de órgãos reguladores do RAPPIBANK, devendo ser atualizada quando for impactada por leis e/ou regulamentos locais, buscando ao máximo não comprometer os requisitos do RAPPIBANK. Esta Política e a documentação associada deverão ser objeto de revisão, pelo menos uma vez por ano, ou de acordo com as necessidades da empresa.

O não cumprimento desta Política poderá gerar sanções disciplinares e eventual inconformidade deve ser relatado imediatamente ao Departamento de Conformidade de Segurança.

4.1 ESTRUTURA ORGANIZACIONAL

A organização de segurança é estabelecida e mantida de acordo com as melhores práticas, assegurando que as responsabilidades seja claramente definidas e atribuídas para apoiar a implementação eficaz de um modelo de segurança contínuo ao longo do tempo.

4.2 USO DE ATIVOS DE INFORMAÇÃO

O uso aceitável de ativo de informação do RAPPIBANK está previsto nesta Política e visa a garantir a segurança e o uso apropriado dos recursos de informação de toda a organização.

4.3 CREDENCIAIS E SENHAS DE ACESSO

Cada usuário é responsável por manter suas credenciais confidenciais e intransferíveis, sendo proibido o compartilhamento de senhas.

A forma de acesso está prevista na Política e o descumprimento dessas regras é considerada uma infração grave, sujeita a medidas conforme previsto na Política de Gestão de Incidentes de Segurança da Informação. Essas medidas visam a garantir a segurança das credenciais e a integridade da informação.

4.4 INTERNET, E-MAIL E MENSAGENS INSTANTÂNEAS

É proibido o envio ou visualização de materiais que violem o Código de Ética ou padrões de bom senso, bem como a distribuição de conteúdo impróprio ou spam. Os remetentes são responsáveis pelas informações enviadas via e-mail e o uso de contas de e-mail pessoais é restrito e não deve interferir nas atividades diárias. Anexos de e-mails não devem ser executados e o acesso a sites relacionados a atividades criminosas na web é proibido, exceto para pessoal autorizado de Segurança de Operações (SecOps). A empresa reserva-se o direito de monitorar e bloquear o tráfego da Internet, se necessário. A transferência de informações de trabalho deve ocorrer apenas por meio de serviços, aplicativos e programas de mensagens instantâneas autorizados. A troca de dados sensíveis requer autorização adequada do proprietário dos dados. Essas diretrizes visam a proteger a integridade das comunicações e informações da empresa.

4.5 CLASSIFICAÇÃO DE INFORMAÇÕES

Todas as informações de negócios do RAPPIBANK ou que circulem dentro do ambiente da empresa são classificados de acordo com seu nível de confidencialidade, integridade e

disponibilidade para poder identificar a criticidade para os negócios de toda a organização.

4.6 PROCESSANDO INFORMAÇÃO

Esta Política e as demais políticas relacionadas, bem como os procedimentos de gestão de informações são estabelecidos de forma segura pelo RAPPIBANK, a fim de preservar a segurança no armazenamento, processamento, transferência ou destruição dessas informações.

4.7 GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

O processo de análise e classificação de riscos é realizado de forma adequada, identificando ameaças e vulnerabilidades relacionadas às informações.

4.8 MONITORAMENTO E RASTREABILIDADE DE ACESSO AOS SISTEMAS

O acesso aos sistemas é registrado, monitorado e cumpre períodos de retenção apropriados e verificados para garantir a conformidade com as políticas de acesso.
Todas essas atividades de monitoramento são consistentes com os regulamentos e legislação de privacidade vigentes em cada um dos sites onde o RAPPIBANK opera.
O time de SECOPS é o responsável por definir os objetivos de controle e o seu âmbito de forma a garantir a mitigação dos riscos associados.

4.9. BACKUPS

O RAPPIBANK implementa diretrizes para garantir a disponibilidade das informações, por meio da execução periódica de cópias de backup dos bancos de dados, instâncias e demais infraestruturas que contenham informações. Estas cópias são testadas regularmente, a fim de verificar a sua integridade, caso seja necessário antes de um evento ou incidente.

4.10 SEGURANÇA DE REDE

As redes virtuais são adequadamente gerenciadas e controladas para proteger as informações nos sistemas e aplicações do RAPPIBANK.

- O RAPPIBANK restringe conexões entre redes não confiáveis e quaisquer componentes do sistema no ambiente de escopo PCI.

- É proibido o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de escopo PCI do RAPPIBANK.

4.11. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Os stakeholders internos e externos do RAPPIBANK são obrigados a proteger as informações da empresa e devem reportar qualquer incidente relatado ou suspeito à equipe de SECOPS o mais rápido possível, de acordo com as diretrizes a seguir.

- Reportar ao SECOPS através dos canais oficiais (Slack ou e-mail corporativo), sobre erros observados, fornecendo informações necessárias para a sua análise.
- Reporte aos Responsáveis pela área de segurança da informação, Heads ou TLs de SECOPS através dos canais de comunicação disponibilizados pela empresa.

4.12 GESTÃO DE VULNERABILIDADES

O único pessoal autorizado a executar qualquer tipo de verificação de vulnerabilidades, testes de penetração de sistemas informáticos, redes de Internet ou redes internas é o time de *SECOPS*- RedTeam. Os referidos testes, no caso de serem realizados em terceiros, só poderão ser executados mediante autorização escrita do proprietário do serviço de digitalização para manter o registo desta autorização.

4.13 DESENVOLVIMENTO SEGURO

Todas as soluções tecnológicas implementadas no RAPPIBANK seguem uma metodologia formal de desenvolvimento e manutenção de sistemas seguros, de acordo com políticas e melhores práticas da indústria. Isso envolve considerar requisitos de segurança da informação durante todo o ciclo de vida, desde o projeto até o comissionamento. Os desenvolvedores recebem treinamento em codificação segura e seguem diretrizes de codificação segura. Além disso, os procedimentos operacionais para sistemas seguros devem ser documentados, implementados e compartilhados com todas as partes envolvidas.

5. RESPONSABILIDADES

- **Todos os colaboradores/usuários**
  I. Proteger adequadamente a informação tratada durante o desempenho das suas tarefas.
  II. Aceitar e cumprir as políticas definidas neste documento.

III. Ser responsável por toda a atividade realizada com a sua própria identificação e credenciais de acesso.

IV. Relatar qualquer evento suspeito ou anomalia de segurança que possa levar a um incidente.

- **Jurídico**

Identificar e manter o SECOPS informado sobre a legislação vigente do país e aplicável à segurança da informação.

- **Administração e Jurídico**

Participar da definição das diretrizes para avaliação/contratação de fornecedores e verificação do cumprimento de acordo com os pontos comprometidos em cada contrato.

- **Proprietário dos dados ou proprietário do ativo de informação:**

Classificar a informação de acordo com o seu nível de criticidade e gerir a informação, bem como a segurança das transações associadas aos ativos que compõem as suas operações diárias.

- **Custodiante de dados**

Gerenciar os controles indicados pelos seus titulares e proporcionar a segurança necessária de acordo com o valor que a informação representa.

- **Conselho de Administração/Conselho**

Promoção e aprovação de diretrizes de segurança, garantia de recursos para sua implementação, promoção de uma cultura de segurança de informação para todas as partes envolvidas e a revisão e aprovação contínua da política de segurança. O objetivo é estabelecer e manter um ambiente seguro, garantir a disponibilidade de recursos necessários e promover conscientização sobre segurança em toda a organização.

- **CIO**

Estabelecer relacionamentos com autoridades de segurança da informação, definir e monitorar políticas de segurança, supervisionar perfis de acesso, relatar questões de segurança cibernética à administração, alinhar estratégias de segurança com os objetivos da empresa, cumprir regulamentos, colaborar com auditorias de segurança e treinamento da equipe e, ainda, promover uma cultura de proteção de dados

- **Time de Tecnologia da Informação**

Avaliação e controle de mecanismos de segurança, a resolução de conflitos regulatórios, a supervisão da implementação de estratégias de segurança, a atualização e distribuição de frameworks de segurança, a coordenação de investigações de incidentes,

liderança em programas de conscientização, avaliação de vulnerabilidades, seleção de parceiros seguros, monitoramento constante de mecanismos de segurança, aconselhamento à alta administração, participação na definição de políticas e procedimentos, e o monitoramento da conformidade com os requisitos de segurança. Essas atividades visam garantir a proteção dos ativos de informação e o cumprimento dos requisitos de segurança.

6. HISTÓRICO DE MUDANÇAS

Detalhes de aprovação do revisor da versão de data
29 de novembro de 2023- Versão 1.0