

Versão V

Política de Segurança Cibernética



Corretora de Câ

Pronance Corretora de Cambio LTDA.
CNPJ: 41.560.568/0001-44
Voluntários da Pátria, 463 Curitiba PR
CEP: 80020-000 Tel. 41 3223-8822
www.pronance.com.br
contato@pronance.com.br

	Política de Segurança Cibernética		Página 2 / 6
	Área Responsável Dir. Compliance	Data de Aprovação: 20/01/2024	Data de Revisão: 20/01/2024
Política de Segurança Cibernética			Versão V

Política de Segurança Cibernética

1. OBJETIVO

O PRONANCE estabelece as diretrizes para compor um programa completo e consistente de segurança da informação e riscos cibernéticos, visando:

- Proteger o valor e a reputação da empresa;
- Garantir a confidencialidade, integridade e disponibilidade das informações do PRONANCE, e de informações de terceiros por ela custodiadas, contra acessos indevidos e modificações não autorizadas, assegurando ainda que as informações estarão disponíveis a todas as partes autorizadas, quando necessário;
- Identificar violações de Segurança Cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos, dentre outros;
- Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;
- Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da empresa;
- Conscientizar, educar e treinar os colaboradores por meio de Política Corporativa de Segurança Cibernética, normas e procedimentos internos aplicáveis as suas atividades diárias;
- Estabelecer e melhorar continuamente um processo de Gestão de Riscos de Segurança Cibernética.

2. CONCEITOS

A Segurança Cibernética, constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

Confidencialidade: garantia de que a informação é acessível somente as pessoas autorizadas.

Integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

	Política de Segurança Cibernética		Página 3 / 6
	Área Responsável Dir. Compliance	Data de Aprovação: 20/01/2024	Data de Revisão: 20/01/2024
Política de Segurança Cibernética			Versão V

Riscos Cibernéticos: Riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, desprotegendo dados, redes e sistemas da empresa causando danos financeiros e de reputação consideráveis.

Malwares:

- Vírus: software que causa danos a máquina, rede, softwares e banco de dados;
- Cavalo de Troia: aparece dentro de outro software e cria uma porta para a invasão do computador;
- Spyware: software malicioso para coletar e monitorar o uso de informações;
- Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

Engenharia Social:

- Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento;
- Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
- Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
- Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;
- Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

Fraudes Externas e invasões: Realização de operações por fraudadores, utilizando-se de ataques em contas bancárias, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ataques DDoS e Botnets: Ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos Botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e enviar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

 Pronance <small>Corretora de Câmbio</small>	Política de Segurança Cibernética			Página 4 / 6
	Área Responsável Dir. Compliance	Data de Aprovação: 20/01/2024	Data de Revisão: 20/01/2024	Execução: Oswaldo
Política de Segurança Cibernética				Versão V

3. PRINCÍPIOS

A proteção e privacidade de dados dos clientes refletem os valores do PRONANCE e reafirmam o seu compromisso com a melhoria contínua da eficácia do processo de Proteção de Dados.

Quanto às informações de nossos clientes, são obedecidas as seguintes determinações:

- São coletadas de forma ética e legal, para propósitos específicos e devidamente informados;
- Somente serão acessadas por pessoas autorizadas e capacitadas para o seu uso adequado;
- Poderão ser disponibilizadas a empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossas diretrizes de segurança e privacidade de dados;
- As informações constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais ou contratuais, somente serão fornecidas aos próprios interessados, mediante a solicitação formal, seguindo os requisitos legais vigentes.

4. DIRETRIZES

O cumprimento da Política de Segurança Cibernética é de responsabilidade de todos os colaboradores e dos prestadores de serviços, os quais devem obedecer às seguintes diretrizes:

- Proteger as informações contra acesso, modificações, destruição ou divulgação não autorizada;
- Prover a adequada classificação da informação, sob os critérios de confidencialidade, disponibilidade e integridade;
- Assegurar que os recursos utilizados para o desempenho de sua função sejam utilizados apenas para as finalidades aprovadas pelo PRONANCE;
- Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos;
- Garantir a continuidade do processamento das informações críticas de negócios;
- Atender às leis que regulamentam as atividades do PRONANCE e seu mercado de atuação;
- Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo;

	Política de Segurança Cibernética		Página 5 / 6
	Área Responsável Dir. Compliance	Data de Aprovação: 20/01/2024	Data de Revisão: 20/01/2024
Política de Segurança Cibernética			Versão V

- Comunicar imediatamente à área de Compliance, quaisquer descumprimentos da Política Corporativa de Segurança Cibernética.

5. ESTRUTURA DE GERENCIAMENTO

O gerenciamento de procedimentos e controles de Segurança Cibernética objetivam assegurar que os procedimentos operacionais de segurança sejam desenvolvidos, implementados e mantidos ou modificados de acordo com os objetivos estabelecidos pela Política de Segurança Cibernética.

5.1 Gestão de acessos às informações

Os acessos às informações são controlados, monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente com a aprovação do Diretor de Compliance, e cancelados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço.

5.2 Proteção do ambiente

São constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações que garantem a segurança na infraestrutura tecnológica de redes locais e internet, através de um gerenciamento efetivo no monitoramento, tratamento e respostas aos incidentes, para minimizar o risco de falhas e a administração segura de redes de comunicações, incluindo a gestão de serviços contratados de processamento e armazenamento de dados e informações em nuvem.

5.3 Segurança Física e Lógica

Os equipamentos e instalações de processamento de informação críticas ou sensíveis são mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

Os requisitos de segurança de sistemas de informação são identificados e acordados antes do seu desenvolvimento e/ou de sua implementação, para que assim possam ser protegidos visando a manutenção de sua confidencialidade, integridade e disponibilidade.

Os colaboradores e terceiros do PRONANCE são treinados periodicamente sobre os conceitos de Segurança da Informação, através de um programa efetivo de conscientização.

	Política de Segurança Cibernética		Página 6 / 6
	Área Responsável Dir. Compliance	Data de Aprovação: 20/01/2024	Data de Revisão: 20/01/2024
Política de Segurança Cibernética			Versão V

5.4 Continuidade de Negócios

O processo de gestão de continuidade de negócios, relativo a segurança da informação é implementado para minimizar os impactos e recuperar perdas de ativos da informação, após um incidente crítico, a um nível aceitável, através da combinação de requisitos como operações, funcionários chaves, mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres. Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados de nuvem e os testes previstos para os cenários de ataques cibernéticos.

5.5 Processamento, Armazenamento de dados e Computação em Nuvem

Conforme a Resolução 4.658/2018 do Banco Central do Brasil, para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, o PRONANCE, assegura-se um procedimento efetivo para a aderência às regras previstas na regulamentação em vigor.

6. RESPONSABILIDADE

A Diretoria da PRONANCE se compromete com a melhoria contínua dos procedimentos e controles relacionados nesta Política, os quais devem ser objetos de pautas recorrentes em Comitês internos da empresa.

7. COMUNICAÇÃO

Quaisquer indícios de irregularidades no cumprimento das determinações desta política serão alvo de investigação interna e devem ser comunicadas imediatamente para o endereço de e-mail ouvidoria@pronance.com.br

Atualização: 11/01/2024.

Contato: compliance@pronance.com.br

By: Kulchesky & Cia Compliance - <https://www.kulcheskycompliance.com/>