# DIRETRIZES DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

O conhecimento, em nossa visão, é chave à manutenção de um ambiente cibernético seguro e confiável. Nesse contexto, buscamos, por meio desta carta, compartilhar as linhas gerais das medidas e procedimentos de segurança cibernética adotados pela Ideal ("Diretrizes"), com os quais recomendamos que nossos clientes e usuários busquem se familiarizar.

Recomendamos, em complemento, a leitura dos demais documentos de segurança da informação e cibernética disponíveis em nosso website, como o documento Boas Práticas de Navegação na Internet, que estabelece linhas gerais de segurança da informação para a navegação segura de nossos clientes e usuários.

As Diretrizes podem ser apresentadas conforme a seguir:

**1. Identificação e Autenticação -** mecanismos que garantem a autenticidade e rastreabilidade dos usuários na utilização dos recursos computacionais. Ou seja, tornam possível a identificação dos autores de qualquer ação feita utilizando os sistemas informatizados e meios de comunicação;

**2. Criptografia -** mecanismo de segurança e privacidade que torna determinada comunicação (e.g., textos, imagens, vídeos) ininteligível para quem não tem acesso aos códigos de codificação ou "tradução" da mensagem;

**3. Prevenção e Detecção de Intrusão -** tecnologias projetadas para monitorar toda atividade de entrada e saída de uma rede de dados, identificando quaisquer padrões suspeitos de tráfego que podem indicar uma tentativa de ataque;

**4. Prevenção de Vazamento de Informações -** processos para o controle da informação na sua utilização, compartilhamento e tráfego;

**5. Varreduras para Detecção de Vulnerabilidades -** procedimentos de detecção de eventuais pontos de fragilidade, que, caso explorados, podem comprometer a confidencialidade, a disponibilidade e a integridade das informações de um indivíduo ou empresa;

**6. Proteção contra Softwares Maliciosos -** tecnologias e soluções que visam a garantir que computadores não estejam vulneráveis a ataques de hackers ou infestados por programas maliciosos;

**7. Mecanismos de Rastreabilidade -** monitoramento do tráfego de informações e recursos de processamento, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da segurança cibernética;

**8. Segmentação da Rede -** segregação dos domínios de rede segundo nível de acesso dos dispositivos ali contidos e isolados, o mitiga os riscos de disseminação em caso de comprometimento de parte da estrutura;

**9. Manutenção das Cópias de Segurança -** processo de cópia de dados de um dispositivo de armazenamento a outro, para que possam ser restaurados em caso de perda dos dados originais;

**10. Registro e Análise de Impacto de Incidentes Ocorridos -** processo que visa a gerenciar a ocorrência de incidentes na infraestrutura de tecnologia da informação, com a finalidade de municiar seu monitoramento, correção e melhoria de processos. Consiste, genericamente, em registrar e analisar a causa dos incidentes ocorridos, fornecendo soluções para evitar sua recorrência, minimizando e/ou evitando seu impacto;

**11. Controles de Acesso -** tecnologia e procedimentos que visam a permitir ou negar a utilização de um objeto (uma entidade passiva, como um sistema ou arquivo) por um sujeito (uma entidade ativa, como um usuário ou um processo);

**12. Disseminação da Cultura de Segurança Cibernética -** engajamento interno ativo da Corretora visando a capacitação contínua e conscientização de seus colaboradores, parceiros, clientes e usuários. Inclui a disseminação contínua de informações, atividades de treinamento, aferição de conhecimento dos colaboradores e, de maneira abrangente, uma variedade de mecanismos de governança e processos com vistas a garantir aderência e conformidade.

Para mais detalhes, acesse a POL0401 – Gestão Integrada de Riscos de TI, ou entre em contato conosco através da caixa de contatos ambos disponíveis na página web da Corretora.

À disposição.

**EQUIPE DE SEGURANÇA DA INFORMAÇÂO – IDEAL CTVM**