



Política de Privacidade e Proteção de Dados

Gow Capital Gestão de Recursos e Consultoria LTDA

Julho 2021

1. OBJETIVO

Em concordância com a Lei Federal Geral de Proteção de dados 13.709 de 14 de agosto de 2018 a LGPD, a GOW CAPITAL GESTÃO DE RECURSOS E CONSULTORIA LTDA visa atender as diretrizes mínimas com relação ao tratamento de dados pessoais e se compromete a fazer o tratamento de dados, sejam de seus clientes, colaboradores, fornecedores, parceiros e terceiros, com o mais alto nível de cuidado, confidencialidade e conformidade com a legislação aplicável.

Essa política visa estabelecer as diretrizes para compor o programa de Segurança Cibernética na GOW CAPITAL.

2. RESPONSABILIDADE

A observância das regras e obrigações contidas nesta Política é dever de todos os colaboradores da GOW CAPITAL, incluindo sócios, administradores, colaboradores e estagiários, prestadores de serviço, terceirizados, consultores e demais pessoas físicas ou jurídicas contratadas ou outras entidades, que participem, de forma direta no que diz respeito às recomendações aos clientes, das atividades diárias e negócios, representando a GOW CAPITAL.

O diretor de Risco e Compliance atuará como Gestor de Proteção de Dados, sendo responsável pelos controles que garantam o atendimento das regras e critérios desta Política:

- Canais de Comunicação para aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; Receber Comunicações da Autoridade Nacional e adotar providências;
- Estabelecer e aprimorar os processos de Proteção de Dados e da Privacidade;
- Monitorar incidentes de Segurança Cibernética;
- Implantar controles de Segurança da Informação de acordo com as instruções deste regulamento;
- Acompanhar atualizações nas diretrizes gerais de Proteção de Dados e da Privacidade, implemento-as sempre que necessário;

- Com apoio da área de Tecnologia da Informação, formular procedimentos técnicos de tratamento de incidentes de segurança da informação;
- Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da empresa;
- Providenciar treinamentos aos colaboradores, conscientizando-os das diretrizes de Privacidade, Segurança e Proteção de Dados;
- Fomentar o comprometimento da alta administração com a melhoria contínua dos processos e recursos necessários para a Segurança e Proteção de Dados.

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política, informando qualquer irregularidade ao responsável por Compliance.

3. DIRETRIZES

A Política de Privacidade e Proteção de Dados tem como diretrizes básicas:

- Assegurar a comunicação, de maneira transparente e clara, do tratamento e compartilhamento dos dados, aos seus devidos titulares;
- Coletar e controlar consentimento do tratamento e compartilhamento dos dados, para finalidade determinada, de seus respectivos titulares;
- Garantir a confidencialidade, integridade e disponibilidade dos dados consentidos a GOW CAPITAL;
- Prover a adequada classificação dos dados, sob os critérios de confidencialidade, disponibilidade e integridade;
- Assegurar medidas técnicas e administrativas a fim de proteger dados e sistemas contra acesso indevido, cópia, leitura, modificação, destruição e divulgação não autorizadas;
- Treinar sócios e colaboradores em programas de conscientização e educação em Compliance, Controles Internos e Segurança da Informação;

4. GESTÃO DE RISCO DE PRIVACIDADE E PROTEÇÃO DE DADOS

A Política de Privacidade e Proteção de Dados tem como gestão de risco:

- A adequada proteção dos ativos cibernéticos da GOW, incluídos à rede de sistemas, softwares, websites, equipamentos e arquivos eletrônicos.
- Restrição e controle do acesso e privilégios de usuários remotos e externos;
- Invalidar contas de Colaboradores e prestadores de serviço em seu desligamento;
- Quando necessário, bloquear chaves de acesso de usuários, e, quando necessário, realizar auditoria para verificação de acessos indevidos;
- Excluir ou desabilitar contas inativas;
- Fornecer senhas de contas privilegiadas somente a Colaboradores que necessitem efetivamente de tais privilégios, mantendo-se o devido registro e controle;
- Detectar, identificar, registrar e comunicar ao Diretor de Risco, Compliance e PLD as violações ou tentativas de acesso não autorizadas;
- Nos casos em que tais serviços e controles acima sejam terceirizados, é necessário que as condições contratuais garantam que o prestador de serviço atesta esta proteção;
- Caso necessário, a partir de resultados apresentados nos testes de aderência, revisar tais práticas;
- A GOW dispõe de *firewall* de segurança nos servidores para acesso à sua rede, visando manter o ambiente de trabalho disponível e livre de vírus e acessos indesejados. O sistema de prevenção a ataques de vírus é regularmente atualizado;

O plano de contingência e de continuidade dos principais sistemas e serviços deve ser objeto de testes, visando a reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

4.1 GESTÃO DE ACESSO

Os serviços de rede, internet e correio eletrônico disponíveis na GOW são de sua propriedade exclusiva, sendo permitido o uso moderado para fins particulares, mediante autorização prévia do Diretor de Risco, Compliance e PLD.



A GOW poderá, a qualquer momento, mediante prévia aprovação do Diretor de Risco, Compliance e PLD, e sem obrigação de cientificação prévia:

- Inspeccionar conteúdo e registrar o tipo de uso dos e-mails feitos pelos usuários;
- Disponibilizar esses recursos a terceiros, caso entenda necessário;
- Solicitar aos usuários justificativas pelo uso efetuado.

No caso de mudança de área ou desligamento do Colaborador, a respectiva senha de acesso é imediatamente adaptada para compatibilizar/adequar o acesso, ou cancelada em definitivo, visando ao impedimento de acesso não autorizado pelo ex-Colaborador.

O Diretor de Risco, Compliance e PLD pode definir bloqueio a sites caso necessário. O monitoramento pode ser feito sem necessidade de prévia ciência dos Colaboradores.

O acesso a sites de armazenamento de arquivos em “nuvem” é permitido.

Os equipamentos, ferramentas e sistemas concedidos aos Colaboradores devem ser configurados com os controles necessários para cumprir os requerimentos de segurança aplicáveis à GOW.

Apenas os Colaboradores devidamente autorizados terão acesso¹ às dependências e sistemas a que estiverem liberados, bem como aos arquivos, diretórios e/ou pastas na rede da GOW, mediante segregação física e lógica

1-Quaisquer exceções deverão ser previamente solicitadas ao Diretor de Risco, Compliance e PLD