1. Objetivo e abrangência

A Política de Segurança da Informação estabelece as diretrizes que a DEFENZ adota para proteger as informações próprias, de seus colaboradores, clientes e parceiros contra acesso e compartilhamento indevido, alteração, perda e/ou indisponibilidade.

Ela se aplica aos sócios, administradores, colaboradores, estagiários, consultores, parceiros e prestadores de serviço, que acessem informações ou sistemas da DEFENZ, em qualquer local e em qualquer equipamento, próprio ou da empresa.

Observação:
A DEFENZ revende licenças de antivírus e EDR Bitdefender, faz implantação e presta suporte técnico, em regra de forma remota. Por isso esta política dá atenção especial ao acesso às consoles de gestão e aos ambientes dos clientes.

2. Referências

- Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais, LGPD) e regulamentos da ANPD;
- Política de Privacidade de Dados e LGPD da DEFENZ, publicada no site da empresa;
- Política Código de Conduta Ética e Anticorrupção da DEFENZ;
- ABNT NBR ISO/IEC 27001 e 27002, como referência de boas práticas.

3. Princípios

Toda decisão sobre informação na DEFENZ observa três princípios:

- Confidencialidade: a informação só é acessada por quem tem necessidade e autorização.
- Integridade: a informação é mantida correta e completa, sem alteração indevida.
- Disponibilidade: a informação e os sistemas estão acessíveis a quem precisa, quando precisa.

4. Classificação da informação

- Pública: pode ser divulgada sem restrição, como material do site e apresentações institucionais.
- Interna: de uso dos colaboradores da DEFENZ, como procedimentos, políticas e relatórios de gestão.
- Confidencial: dados de clientes, dados pessoais, credenciais, propostas comerciais, contratos e informações financeiras. Acesso restrito a quem precisa para o trabalho.

Na dúvida, a informação é tratada como Confidencial.

5. Responsabilidades

- Sócia administradora: aprova esta política, garante os recursos para cumpri-la e decide sobre exceções.
- Responsável por Segurança da Informação, designado pela administração: mantém esta política, acompanha seu cumprimento, conduz a resposta a incidentes e responde a clientes e parceiros sobre o tema.
- Colaboradores e prestadores: cumprem esta política, protegem as credenciais pessoais e comunicam imediatamente qualquer suspeita de incidente.

6. Controle de acesso e senhas

- Cada usuário criado é próprio e intransferível, é proibido compartilhar estes dados.
- O acesso é concedido pelo princípio do menor privilégio: apenas o necessário para a função, e revisto quando a função muda.
- A autenticação em dois fatores (MFA) é obrigatória no e-mail corporativo, no CRM e nas consoles de gestão de segurança, sempre que o sistema oferecer.
- Senhas têm no mínimo 12 caracteres, não são reutilizadas entre sistemas e são guardadas em gerenciador de senhas, nunca em planilha, papel ou mensagem.
- No desligamento de colaborador ou fim de contrato de prestador, todos os acessos são revogados, imediatamente, e os equipamentos e dados da empresa são devolvidos durante o processo.

7. Acesso a ambientes de clientes

- O acesso às consoles de gestão Bitdefender e aos ambientes dos clientes é feito apenas para a execução do serviço contratado e por pessoas autorizadas.
- Credenciais fornecidas pelo cliente são tratadas como Confidenciais, usadas somente para a finalidade combinada e nunca reaproveitadas em outro cliente.
- Toda alteração relevante feita no ambiente do cliente é registrada no chamado ou no histórico de atendimento.
- Encerrado o contrato, a DEFENZ remove os próprios acessos e devolve ou elimina as informações do cliente, salvo obrigação legal de guarda.

8. Uso aceitável dos recursos

- E-mail, armazenamento em nuvem, CRM e demais ferramentas da DEFENZ são para uso profissional.
- Informações Confidenciais são armazenadas apenas nos ambientes corporativos aprovados, e não em contas pessoais, pen drives ou aplicativos não autorizados.

- Dados de clientes e dados pessoais não são inseridos em ferramentas de inteligência artificial ou serviços externos sem aprovação do responsável por Segurança da Informação.
- É proibido instalar software sem licença ou de origem desconhecida.

9. Proteção de equipamentos

- Todo equipamento usado para trabalhar na DEFENZ, próprio ou da empresa, tem solução de proteção de endpoint ativa e atualizada, com tela bloqueada por senha e sistema operacional com atualizações em dia.
- Notebooks com informações Confidenciais têm o disco criptografado.
- Perda, furto ou suspeita de comprometimento de equipamento é comunicada imediatamente ao responsável por Segurança da Informação.

10. Cópias de segurança e continuidade

- Os documentos da empresa são mantidos nos serviços corporativos em nuvem, com retenção e possibilidade de recuperação.
- Informações essenciais à operação têm cópia de segurança, e a recuperação é testada periodicamente.

11. Fornecedores e terceiros

Fornecedores e prestadores que tenham acesso a informações Confidenciais da DEFENZ ou de seus clientes assumem por escrito o compromisso de confidencialidade e de cumprimento da LGPD.

12. Incidentes de segurança

- Qualquer suspeita de incidente, como acesso indevido, vazamento, perda de dados ou infecção, é comunicada imediatamente ao responsável por Segurança da Informação.
- A resposta segue o Plano de Ação para incidente de vazamento de dados da Política de Privacidade de Dados e LGPD: contenção, avaliação, comunicação, correção e registro.
- Quando o incidente envolver dados de cliente, o cliente é informado sem demora. Quando houver risco ou dano relevante aos titulares, a comunicação à ANPD e aos titulares segue o prazo da regulamentação vigente.

13. Conscientização

Todo colaborador recebe esta política na entrada e participa de orientação periódica sobre segurança da informação, com foco em golpes por e-mail, engenharia social e proteção de senhas.

14. Descumprimento

O descumprimento desta política sujeita o responsável às medidas disciplinares e contratuais cabíveis, sem prejuízo das responsabilidades civis e criminais.

15. Revisão

Esta política é revista no mínimo uma vez por ano, ou antes, quando houver mudança relevante no negócio, na legislação ou após incidente.