

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – VERTEX

1. Introdução

A segurança da informação na Vertex é um pilar estratégico. Esta política estabelece diretrizes claras para proteger a confidencialidade, integridade, disponibilidade e legalidade das informações corporativas. Está alinhada à Lei Geral de Proteção de Dados (LGPD – Lei 13.709/2018) e às melhores práticas do mercado.

2. Aplicabilidade

Esta política aplica-se a todos os colaboradores, prestadores de serviço, parceiros, sistemas e ambientes que interajam com ativos e informações da Vertex, incluindo acessos remotos ou terceirizados.

3. Objetivos

- Garantir proteção integral às informações corporativas;
- Prevenir perdas financeiras, operacionais e reputacionais;
- Manter conformidade legal e contratual;
- Promover uma cultura de segurança e responsabilidade digital.

4. Deveres e Responsabilidades

- Todos devem tratar a informação como ativo estratégico e seguir esta política;
- O setor de TI é responsável pela criação, manutenção e auditoria dos controles;
- Incidentes devem ser reportados imediatamente para: contato@vertexrc.com.br

5. Monitoramento e Auditoria

A Vertex poderá:

- Monitorar acessos, e-mails, redes e dispositivos;
- Implantar trilhas de auditoria e logs;
- Utilizar ferramentas de prevenção contra ameaças internas e externas.

6. Uso e Classificação da Informação

- Informações são classificadas em: Públicas, Internas, Restritas e Confidenciais;
- É vedado divulgar ou compartilhar dados sem autorização expressa;

- Informações confidenciais devem ser protegidas mesmo após o término do vínculo.

7. Dados de Terceiros e Compartilhamento

- A Vertex armazena e processa dados de terceiros somente quando necessário ao negócio;
- O compartilhamento exige contrato, cláusulas de confidencialidade e base legal;
- Proíbe-se o armazenamento local de dados críticos – uso obrigatório de armazenamento seguro na nuvem.

8. Programas e Propriedade Intelectual

- É proibido o uso de softwares não licenciados;
- Apenas o TI pode instalar programas;
- Toda criação ou inovação feita sob vínculo empregatício pertence à Vertex.

9. Controle de Acesso e Senhas

- Acesso é individual, intransferível e controlado por autenticação forte;
- Senhas devem ser complexas e atualizadas regularmente;
- Compartilhamento de credenciais é proibido.

10. Internet e Correio Eletrônico

- Uso restrito a fins profissionais;
- É proibido acessar conteúdo impróprio ou ilegal;
- E-mails devem ser profissionais e auditáveis;
- Mensagens ofensivas, difamatórias ou ilegais serão punidas.

11. Acesso Remoto (VPN)

- O uso de VPN exige autorização da direção;
- Relatórios de acesso remoto são auditados;
- Devem ser utilizados apenas para atividades profissionais.

12. Armazenamento e Backup

- Backups são automatizados e monitorados;
- É proibido uso de mídias removíveis ou armazenamento pessoal não autorizado;
- Restores devem ser formalizados via sistema interno de chamados.

13. Segurança Física e “Mesa Limpa”

- Informações sensíveis devem ser guardadas em armários seguros;

- Nenhum dado deve ser deixado em mesas, quadros ou impressoras;
- Computadores devem ser bloqueados quando fora de uso.

14. Pentest e Gestão de Vulnerabilidades

- Testes de intrusão devem ser realizados anualmente;
- Devem seguir boas práticas e proteger a confidencialidade das informações testadas.

15. Aplicações em Nuvem

- Serviços em nuvem devem possuir cláusulas contratuais de segurança;
- A Vertex deve exigir gestão de vulnerabilidades do provedor.

16. Conscientização e Treinamento

- Todos os colaboradores participam de treinamentos anuais de segurança da informação;
- A cultura de proteção de dados deve ser reforçada continuamente.

17. Continuidade de Negócios

- Planos de continuidade são mantidos, testados e atualizados;
- Devem garantir a operação mesmo em cenários críticos ou desastres.

18. Penalidades

O descumprimento desta política constitui falta grave e poderá resultar em sanções administrativas, civis e penais.

Canais de denúncia:

- Online: vertexrc.com.br/canal-de-denuncias
- Telefone: (41) 3163-6464

19. Revisão

Esta política será revisada anualmente ou em caso de alteração regulatória significativa.