VidyAccess

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

Esta política estabelece os fundamentos, as responsabilidades e as diretrizes que norteiam o tratamento das informações da VidyAccess, garantindo que todos os dados e ativos sejam manejados de forma segura, ética e alinhada aos objetivos estratégicos da organização.

2. ABRANGÊNCIA

Aplica-se a todos os colaboradores, estagiários, fornecedores, parceiros, prestadores de serviço e demais partes interessadas que tenham acesso às informações ou aos ambientes físicos e lógicos da VidyAccess.

3. REFERÊNCIAS NORMATIVAS E LEGAIS

- ABNT NBR ISO/IEC 27002:2023 — Tecnologia da Informação — Código de prática para controles de segurança;
- ABNT NBR ISO/IEC 27014 — Governança de segurança da informação;
- Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD);
- Código de Ética e Conduta da VidyAccess;
- Política de Privacidade da VidyAccess.

4. TERMOS E DEFINIÇÕES

- **Informação**: É a reunião ou conjunto de dados e conhecimentos resultante do processamento, manipulação e/ou organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (humano ou máquina) que a recebe;
- **Segurança da Informação (SI)**: conjunto de processos, práticas e controles destinados a preservar a confidencialidade, integridade, disponibilidade, autenticidade e conformidade das informações;
- **Confidencialidade**: garantia de que apenas pessoas autorizadas têm acesso às informações;
- **Integridade**: salvaguarda da exatidão e da confiabilidade das informações e de seus métodos de processamento;

- **Disponibilidade**: garantia de que usuários autorizados obtenham acesso às informações e ativos quando necessário;
- **Conformidade**: adesão a requisitos legais, regulatórios, contratuais e a políticas internas;
- **Incidente de SI**: evento que comprometa ou ameace comprometer qualquer um dos pilares da segurança da informação;
- **Risco de SI**: possibilidade de ocorrência de incidentes que resultem em impacto negativo para a organização.

5. PRINCÍPIOS E DIRETRIZES

A VidyAccess adota as seguintes diretrizes para proteger seus ativos de informação:

- Assegurar que terceirizados, contratados, consultores e temporários realizem o **treinamento obrigatório de segurança da informação** da VidyAccess e atuem em conformidade com a legislação, normas e padrões locais vigentes;
- Preservar a confidencialidade, integridade e disponibilidade das informações por meio de controles adequados e proporcionais aos riscos identificados;
- Proteger sistemas e dados contra acesso, alteração, destruição ou divulgação não autorizados;
- Garantir que os ativos de informação sejam utilizados exclusivamente para finalidades aprovadas, estando sujeitos a auditoria e monitoramento;
- Promover programas contínuos de conscientização e capacitação em segurança da informação;
- Assegurar que cada pessoa, independentemente de vínculo ou nível hierárquico, seja responsável por zelar pelos dados e ambientes aos quais tem acesso através.

5.1 Proteção da Informação

Todas as informações geradas ou recebidas pela VidyAccess são propriedade da organização e devem ser protegidas contra riscos e ameaças internas e externas que possam comprometer a confidencialidade, integridade ou disponibilidade destas. A empresa reserva-se o direito de restringir, monitorar e controlar o acesso a tais recursos.

5.2 Monitoramento

A Área de Segurança da Informação pode, quando julgar necessário, monitorar equipamentos, redes e sistemas para preservar a segurança corporativa. Isso inclui análise de tráfego, e-mails, diretórios e documentos impressos deixados em locais de acesso público.

5.3 Classificação da Informação

Para orientar o manejo adequado, as informações são categorizadas em quatro níveis:

- Confidencial — divulgação altamente restrita.
- Restrita — uso limitado a grupos específicos.
- Uso Interno — acesso permitido a todos os colaboradores.
- Pública — sem restrição de acesso.

5.4 Gestão de Continuidade de Negócios

Estabelecer o direcionamento estratégico necessário à Gestão de Continuidade de Negócios da VidyAccess, para planejar respostas a eventos que tragam interrupção das operações, provendo a continuidade dos produtos e críticos prestados aos clientes e cooperados, bem como a retomada destes produtos e serviços à operação normal.

5.5 Gestão de Identidades e Acessos

O acesso a sistemas e informações deve ser concedido apenas a pessoas autorizadas, mediante aprovação formal, e limitado ao mínimo necessário ao desempenho de suas funções.

5.6 Tratamento de Informações Confidenciais

Documentos confidenciais devem ser protegidos por senha ou criptografia e não podem ser compartilhados sem autorização expressa. Suspeitas de uso indevido devem ser reportadas imediatamente ao encarregado/DPO (dpo@vidyaccess.com).

5.7 Armazenamento de Dados

Informações corporativas devem ser armazenadas em repositórios oficiais da VidyAccess com backup automático. É proibido utilizar serviços de armazenamento pessoais ou não autorizados.

5.8 Credenciais de Acesso

- A senha é pessoal e intransferível;
- Deve conter ao menos 8 caracteres, combinando letras maiúsculas, minúsculas, números e símbolos;
- Mudança obrigatória a cada 90 dias, sem reutilizar as três últimas senhas.

5.9 Uso de Recursos Computacionais, Software e Licenças

- A instalação de software depende de autorização da Área de SI.
- Somente softwares licenciados à VidyAccess podem ser utilizados.
- Softwares gratuitos deverão ser homologados previamente.

5.10 Violações e Medidas Disciplinares

São consideradas violações diretas as regras gerais de segurança da VidyAccess:

- Mostrar, armazenar ou transmitir texto, imagens ou sons que possam ser considerados ofensivos, abusivos, pornográficos, racistas, difamatórios ou ilegais;
- Efetuar ou tentar qualquer tipo de acesso não autorizado aos recursos computacionais da empresa;
- Utilizar os recursos computacionais da Empresa para acesso não autorizado a recursos de terceiros;
- Violar ou tentar violar os sistemas de segurança, quebrando ou tentando adivinhar a identidade eletrônica de outro usuário, senhas ou outros dispositivos de segurança, interferindo em qualquer equipamento ou sistema de segurança;
- Atos de mau uso dos recursos computacionais e que violem as regras de uso dos recursos computacionais descritas neste documento;
- Desse modo, as violações e o não cumprimento da Política de Segurança da Informação estabelecida, estão sujeitas às sanções disciplinares e penalidades previstas no Código de Conduta da VidyAccess, e se for o caso, o infrator estará sujeito à legislação pertinente do Código Penal Brasileiro.

5.11 Boas Práticas Gerais

As seguintes práticas devem ser adotadas em ambientes de trabalho remotos e externos:

- **Treinamento / Conformidade Legal** — antes de iniciar qualquer projeto ou trabalho, **é obrigatório** que colaboradores, terceirizados, contratados, consultores e temporários realizem o treinamento de segurança da informação da VidyAccess e atuem em conformidade com a legislação, normas e padrões locais vigentes;
- Documentos impressos —nunca deixe documentos confidenciais expostos em locais com possível acesso de pessoas que não estejam alocadas no projeto;
- Impressões — avalie a real necessidade antes de imprimir documentos de projetos e guarde em locais privados quaisquer documentos com informações de projetos;
- Bloqueio de Tela — bloqueie seu dispositivo sempre que se afastar;
- Conversas e Registros de Informações — não discutir assuntos confidenciais em ambientes públicos ou inadequados, especialmente na presença de pessoas não envolvidas diretamente no projeto
- Cópias — não copiar ou reproduzir documentos ou qualquer tipo de informação sem expressa autorização do setor responsável pela sua guarda;
- Armazenamento Adequado — salvar e armazenar os arquivos pertinentes a assuntos da Empresa nos servidores de arquivos de sua área, conforme orientação dos Responsável por Tecnologia da Informação (TI), respeitando as peculiaridades de confidencialidade e guarda de cada projeto e exigência de nossos clientes e parceiros;
- Uso de Equipamentos — utilizar equipamentos de informática somente com a autorização expressa da sua gestão e com a orientação do setor de suporte ao usuário;
- Patrimônio — cuide adequadamente dos equipamentos fornecidos, no caso do notebook, nunca deixar exposto em local inseguro como carros, malas, mochilas sem a sua devida supervisão;

- Notificação de Incidentes — no caso de identificar qualquer incidente de segurança da informação, o fato deve ser imediatamente notificado para o DPO através do e-mail dpo@vidyaccess.com

5.12 Princípios Fundamentais

O compromisso com o tratamento adequado das informações da VidyAccess, clientes, prestadores de serviço e do público em geral está fundamentado nos seguintes princípios:

- Confidencialidade: garantir que o acesso à informação seja somente por pessoas autorizadas e quando de fato necessário;
- Integridade: garantir que as informações sejam mantidas íntegras, sem modificações indevidas sejam acidentais ou propositais;
- Disponibilidade: garantir que as informações estejam disponíveis a todas as pessoas autorizadas a acessá-las.

5.13 Atualizações da Política

Esta política poderá ser revista e atualizada sempre que necessário para refletir mudanças legais, tecnológicas ou organizacionais.

6. Papéis e Responsabilidades

- Diretoria — a Política de Segurança da Informação ressalta o comprometimento da direção organizacional da VidyAccess com vistas a garantir a implementação das diretrizes e princípios da segurança da informação da VidyAccess. A Diretoria é responsável por assegurar a capacitação e monitoramento dos usuários para que atuem sempre em conformidade com a política de segurança da informação da VidyAccess, refletindo a legislação, normas e padrões locais vigentes;
- Usuários — é dever e responsabilidade de cada usuário — incluindo colaboradores, estagiários, terceiros, fornecedores e parceiros, independentemente do vínculo, função ou nível hierárquico — proteger e zelar pelos ativos e informações aos quais tenham acesso ou contato, bem como pelos ambientes físicos e computacionais utilizados. Essa responsabilidade deve ser exercida independentemente das medidas de segurança implantadas e sempre em conformidade com a política de segurança da informação da VidyAccess, refletindo a legislação, normas e padrões locais vigentes.

7. CONTATO

Dúvidas ou relatos de incidentes devem ser encaminhados para: dpo@vidyaccess.com

Atenciosamente,

Rafaeli Lemos de Souza
Diretora Estatutária - DPO
dpo@vidyaccess.com

Versão 1
Data de atualização: 07/07/2025