POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

Esta política de segurança da informação tem como objetivo proteger a confidencialidade, a integridade e a disponibilidade das informações que circulam na SevenX, garantindo a conformidade com as regulamentações aplicáveis e promovendo a segurança em todas as operações da plataforma de apostas.

Além disso, visa fornecer diretrizes relacionadas ao manuseio, controle e descarte das informações, promovendo a melhoria contínua dos processos de segurança da informação.

2. APLICAÇÃO

Esta política se aplica a todos os prestadores, parceiros e sistemas da SevenX que manuseiam informações sensíveis, abrangendo dados de clientes, prestadores, transações financeiras e informações estratégicas.

3. REFERÊNCIA

- Lei nº 13.709 (“Lei Geral de Proteção de Dados”)
- Lei nº 14.790 (“Lei Geral de Apostas”)
- Portaria nº 827;
- Código de Ética e Conduta;
- Política de Governança e Compliance;
- Política de Gerenciamento de Riscos e Controles Internos;
- Política de Privacidade e Proteção de Dados Pessoais.

4. CONCEITOS

Para fins desta política são observados os seguintes conceitos:

Acesso Conflitante	Situação em que o usuário possui permissões ou privilégios que entram em conflito com as políticas da organização, podendo resultar em vulnerabilidade ou riscos de segurança.
Ativo de Informação	Dados ou informações que possuem valor à organização. Ativos de informação podem incluir bancos de dados, documentos, e-mails, planilhas e qualquer outro meio onde a informação seja armazenada, processada e utilizada.
Ativo de Tecnologia	Recursos tecnológicos que suportam o processamento, armazenamento e a comunicação de informações. Inclui hardware como servidores, computadores, dispositivos móveis, redes e software, incluindo sistemas operacionais e aplicativos.
Ciclo de Vida	Recebimento, manuseio, transporte, armazenamento ou descarte de informações.
Gestor, Criador de	Pessoa ou entidade responsável pela geração ou produção de dados e

Informação	informações dentro de um contexto específico.
Inventário de Ativos	Registro detalhado de todos os recursos de todas as propriedades, tanto físicas quanto digitais, de uma entidade, utilizado para gerenciar e manter o controle eficiente dos ativos.
Rede de Dados	Infraestrutura que possibilita a comunicação e troca de informações, abrangendo tanto componentes físicos (hardware) quanto os elementos lógicos (software).
Sistemas Corporativos	Conjunto integrado de aplicativos e tecnologias utilizado por uma empresa para suportar suas operações e seus processos de negócios.
Usuário	Indivíduos que interagem com um sistema, um aplicativo, uma plataforma, para realizar tarefas específicas.

5. PRINCÍPIOS

Os princípios de confidencialidade, integridade e disponibilidade norteiam todas as ações da SevenX e são fundamentais para a política de segurança da informação.

Princípios	**Descrição**	**Práticas - SevenX**
Confidencialidade	A confidencialidade é crucial para proteger dados pessoais, segredos comerciais e informações estratégicas, evitando vazamentos que possam resultar em prejuízos financeiros ou reputacionais Assegurar que a informação seja acessível apenas por pessoas autorizadas.	Criptografia, controle de acesso, autenticação forte e políticas de classificação de informações
Integridade	Garantir que a informação esteja precisa e completa, protegendo-a contra modificações não autorizadas. Manter a integridade dos dados é vital para a confiança nas informações utilizadas para a tomada de decisões, relatórios financeiros e operações diárias.	Auditoria de dados e controles de acesso.

Disponibilidade	Assegurar que a informação esteja acessível e utilizável quando necessário. Isso envolve a proteção contra interrupções e falhas. A disponibilidade é crítica para o funcionamento contínuo de uma organização. Interrupções podem afetar a produtividade, a confiança dos clientes e a capacidade de cumprir obrigações legais.	Redundância de sistemas, backups regulares, manutenção preventiva e planos de recuperação de desastres

RESPONSABILIDADES

A segurança da informação é uma responsabilidade compartilhada por todos na empresa. Cada prestador desempenha um papel essencial, seja no uso adequado de senhas, no compartilhamento consciente de informações ou na proteção de dados sensíveis. É fundamental que todos estejam alinhados às melhores práticas e políticas de segurança, contribuindo para um ambiente seguro e protegendo não apenas as informações da empresa, mas também a confiança de nossos clientes e parceiros.

Embora a responsabilidade seja coletiva, é crucial que cada parte cumpra seu papel para garantir a eficácia desta política:

- Gestão: Assegurar que todos os recursos necessários para a implementação e manutenção da segurança da informação sejam disponibilizados.
- prestadores: Cumprir as diretrizes da política e participar de treinamentos regulares sobre segurança da informação.
- Equipe de TI: Implementar controles técnicos e monitorar os sistemas para prevenir e responder a incidentes de segurança.

6. DIRETRIZES

6.1 Classificação da Informação:

Os ativos de informação que circulam na empresa devem ser classificados nas seguintes categorias: Pública, Interna, Confidencial e Restrita. Essa classificação orienta o tratamento e a proteção das informações, assegurando a confidencialidade, integridade e disponibilidade dos dados e sistemas utilizados.

- O acesso às informações é restrito aos prestadores cujas funções exigem seu uso.
- Os documentos produzidos no ambiente da SevenX devem ser classificados pelo criador (gestor) de acordo com seu conteúdo.
- O uso dos recursos e ativos corporativos pode ser monitorado, sendo proibido o uso para atividades não relacionadas às funções desempenhadas.
- Todos os prestadores devem assinar um termo de responsabilidade e confidencialidade, que será armazenado no RH.

6.2 Gestão do Acesso:

A SevenX adota medidas de segurança rigorosas para controlar o acesso à rede, sistemas operacionais, aplicações e informações sensíveis.

- Isolamento de Sistemas Sensíveis: Os sistemas críticos são isolados, e o acesso a informações é autorizado apenas pela área responsável, com base nas funções do usuário.
- Autenticação: Todos os usuários devem ser identificados, autenticados e autorizados para acessar os sistemas. As ações realizadas poderão ser auditadas a qualquer momento.
- Acesso de Terceiros: Não é permitido acesso a usuários ou entidades externas sem autorização formal do gestor de segurança.
- Uso do E-mail Corporativo: O e-mail e as informações enviadas por esse meio pertencem à SevenX e devem ser utilizados exclusivamente para atividades profissionais.
- Senhas: As senhas são pessoais, intransferíveis e de responsabilidade exclusiva do usuário, devendo seguir regras mínimas de complexidade e não ser compartilhadas.
- Revisão de Acessos: Os acessos serão revisados regularmente para inativação de usuários indevidos e ajuste de permissões excessivas.

1. **Proteção Contra Ameaças**

- Treinamento: prestadores são capacitados para identificar tentativas de phishing e outros ataques cibernéticos, como engenharia social.
- Infraestrutura de Segurança: A empresa utiliza soluções atualizadas de firewall e antivírus para proteger sua infraestrutura contra ameaças internas e externas.

2. **Segurança em Transações**

- Criptografia: As transações operacionais e dados pessoais dos usuários são protegidos por criptografia.
- Monitoramento: Há monitoramento em tempo real para detectar e responder a atividades suspeitas.
- Inventário: Um inventário de ativos tecnológicos é mantido e atualizado sempre que necessário.

6.3 Gestão de Incidentes

A SevenX possui um plano de resposta a incidentes, com procedimentos claros para identificar, responder e recuperar-se de incidentes de segurança.

- Notificação: A alta direção e o DPO (Encarregado de Proteção de Dados) são imediatamente notificados em caso de incidente.

6.4 Avaliação de Riscos

- **Análises Regulares:** Avaliações de risco são realizadas para identificar vulnerabilidades e definir medidas corretivas eficazes.
- **Testes de Penetração:** Testes de penetração são conduzidos anualmente para avaliar a segurança da infraestrutura de TI.

6.5 Compliance e Regulamentação

- A empresa mantém-se atualizada em relação às regulamentações do setor e garante que suas práticas estejam em conformidade com as leis e diretrizes aplicáveis.

6.6 Proteção de Dados

- **Criptografia:** Implementação de criptografia para proteger informações sensíveis em trânsito e em repouso.
- **LGPD:** Garantia de que os dados pessoais de clientes sejam coletados, armazenados e processados de acordo com a LGPD e outras regulamentações aplicáveis.

7. GESTÃO DE INCIDENTES

- **Processo de Resposta:** Estabelecimento de processos para identificar, relatar e responder a incidentes de segurança.
- **Análises Pós-Incidente: Realização de análises pós-incidente para aprimorar os controles de segurança.**

8. TREINAMENTO E CONSCIENTIZAÇÃO

- **Treinamentos Regulares:** Todos os prestadores participam de treinamentos sobre segurança da informação.
- **Cultura de Segurança:** A empresa promove uma cultura de segurança, incentivando a comunicação aberta sobre riscos e incidentes.
- **Consequências:** O não cumprimento desta política pode resultar em ações disciplinares e implicações legais.

9. CONCLUSÃO

A segurança da informação é uma responsabilidade compartilhada por todos os prestadores da SevenX. É fundamental que cada membro da equipe compreenda e siga essa política, contribuindo para um ambiente seguro e protegendo tanto o negócio quanto a confiança de nossos usuários e parceiros.

10. REVISÃO E APROVAÇÃO

Esta política será revisada anualmente pela alta administração da SevenX, garantindo conformidade.

Data	Andamento	Responsável
15/10/2024	**1ª Versão**	Analista de Compliance
20/10/2024	**Validação**	Gerente de Compliance, Integridade e Riscos
18/11/2024	**Aprovação**	Presidência