AVENUE

Política de Segurança da Informação e Cybersecurity

Índice

AVENUE

1. Objetivo

O objetivo deste documento é estabelecer a Política de Segurança da Informação e Segurança Cibernética da Avenue Holding Inc. e de todas as empresas que fazem parte de seu grupo, incluindo subsidiárias, empresas controladoras e afiliadas (todas em conjunto ou individualmente, referidas como Avenue), visando a Confidencialidade, Integridade e Disponibilidade das informações da Avenue e daquelas que estão sob sua custódia.

2. Introdução

A política descreve as diretrizes e a conduta adequada para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados (acidentais ou intencionais).

O detalhamento das diretrizes aqui dispostas serão objetos de normas e procedimentos específicos compondo o Sistema de Gestão de Segurança da Informação e Segurança Cibernética.

3. Público-Alvo

Todos os administradores, sócios, funcionários e estagiários, consultores, prestadores de serviço ou qualquer terceiro que trabalhe para ou em nome da Avenue (Colaboradores) estão sujeitos ao cumprimento dos termos desta Política e outros procedimentos relacionados à segurança da informação, independentemente de cargo, departamento ou função.

4. Princípios da Segurança da Informação

Nosso compromisso com o tratamento adequado das informações da Avenue, clientes e público em geral está fundamentado nos seguintes princípios:

4.1 Confidencialidade

Garantimos que o acesso à informação seja obtido somente por pessoas autorizadas e quando ele for de fato necessário.

4.2 Disponibilidade

Garantimos que as pessoas autorizadas tenham acesso à informação sempre que necessário.

4.3 Integridade

Garantimos a exatidão e completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos.

5. Diretrizes

A segurança da informação na Avenue estabelece as seguintes diretrizes:

- As informações da Avenue, dos clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida.
- A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.
- O acesso às informações e recursos só deve ser feito se devidamente autorizado.
- A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.
- A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades.
- A credencial de acesso é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.
- Todo colaborador deve reportar os riscos às informações à área de Segurança da Informação.
- A área de Segurança de Informação deve divulgar amplamente as responsabilidades sobre Segurança da Informação aos Colaboradores, que devem entender e assegurar estas diretrizes.

6. Processos de Segurança da Informação

Para assegurar que as informações tratadas pela Avenue estejam devidamente protegidas, adotamos processos de segurança da informação que contemplam os seguintes tópicos:

6.1 Gestão de Ativos

Entende-se por ativos da Informação tudo o que pode criar, processar, armazenar, transmitir e até excluir a informação. Podem ser tecnológicos (software e hardware) e não tecnológicos (pessoas, processos e dependências físicas).

Os ativos da informação devem ser classificados e protegidos contra acessos indevidos de acordo com seu grau de risco. As proteções devem contemplar medidas de segurança física e lógica, incluindo: hardening, gestão de patches, mecanismos de autenticação/autorização e identificação de vulnerabilidades.

6.2 Gestão de Acessos

As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos da Avenue.

Os acessos devem ser rastreáveis, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente o Colaborador, para que seja responsabilizado por suas ações.

6.3 Classificação da Informação

As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Restrita, Confidencial, Interna e Pública. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

6.4 Gestão de Riscos

Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação da Avenue, para que sejam recomendadas as proteções adequadas.

Os cenários de riscos de segurança da informação são escalonados nos fóruns apropriados, para decisão.

A Avenue contrata seguro cibernético, para minimizar impactos financeiros decorrentes e eventuais incidentes de segurança da informação.

6.5 Gestão de Riscos em Prestadores de Serviços

Os prestadores de serviços contratados pela Avenue são classificados considerando critérios, tais como, mas não se limitando:

- Criticidade do segmento;
- Informações mais críticas manipuladas pelo fornecedor;
- Forma de acesso às informações;
- Certificações;
- Análise feita através da Due Diligence.

Dependendo da classificação, o prestador deverá passar por avaliação de risco, que vai desde a validação in loco dos controles de Segurança da Informação, avaliação remota das evidências ou outros processos de avaliação, além do acompanhamento de eventuais correções e melhorias implementadas pelos prestadores de serviços.

6.6 Gestão de Incidentes de Segurança da Informação e Cybersecurity

A área de Cybersecurity realiza o monitoramento de segurança do ambiente tecnológico da Avenue, analisando os eventos e alertas com o objetivo de identificar possíveis incidentes.

Os incidentes que são identificados pelos alertas são classificados com relação ao impacto de acordo com os critérios adotados pela Avenue.

6.7 Conscientização e Treinamento

Todos os colaboradores e terceiros devem ser conscientizados e treinados quanto às melhores práticas de segurança da informação de forma a compreender o seu papel e responsabilidade, com o objetivo de fortalecer a cultura e a proteção das informações da Avenue, de seus clientes e parceiros.

Periodicamente, são disponibilizadas campanhas de conscientização ou treinamentos que podem ser presenciais ou on-line, relacionados a confidencialidade, integridade e disponibilidade da informação. Estas campanhas são veiculadas através de e-mails, portal corporativo, e-learning, mídia indoor, redes sociais aos colaboradores e clientes.

6.8 Governança com as áreas de Negócio e Tecnologia

As iniciativas e projetos das áreas de negócio e tecnologia devem estar alinhadas com as diretrizes e arquiteturas de segurança da informação, garantindo a confidencialidade, integridade e disponibilidade das informações.

6.9 Segurança Física do Ambiente

O processo de Segurança Física visa estabelecer controles relacionados à concessão de acesso físico ao ambiente somente a pessoas autorizadas, de acordo com a criticidade das informações previamente mapeadas.

6.10 Desenvolvimento Seguro de Sistemas

O processo de desenvolvimento de sistemas de aplicação deve garantir a aderência às políticas de segurança da Avenue e às boas práticas de segurança.

6.11 Gestão de Mudança

A gestão de mudança deve evitar ou minimizar qualquer indisponibilidade nos serviços, produtos ou sistemas utilizados pela Avenue.

O processo gestão de mudança irá analisar as mudanças necessárias para que não impactem um ou mais pilares de segurança: confiabilidade, integridade e disponibilidade.

6.12 Gravação de Logs

É obrigatória a gravação de logs ou trilhas de auditoria do ambiente computacional de forma a permitir identificar: quem fez o acesso; quando o acesso foi feito; o que foi acessado e como foi acessado.

As informações dos registros (logs) ou trilhas de auditoria devem ser protegidas contra modificações e acessos não autorizados.

6.13 Proteção de Rede e Perímetro

Para proteção da infraestrutura da Avenue contra um ataque externo, utilizamos ferramentas e controles contra: ataques que afetem a disponibilidade (DDoS), Spam, Phishing, Malware, invasão de dispositivos de rede e servidores, ataques de aplicação e scan externos.

Para acesso dos Colaboradores aos sistemas e redes da Avenue, adotamos princípios zero trust com múltiplos fatores de validação de credencias, dispositivos e contexto do acesso.

6.14 Proteção da Informação

A informação pode estar presente de diversas formas, tais como: sistemas, drives locais e em nuvem, banco de dados, mídia impressa, dispositivos eletrônicos, equipamentos, comunicação oral, dentre outros.

Independente da forma, toda informação gerada, adquirida, armazenada e/ou processada, pela Avenue ou através de parceiros de negócio e/ou prestadores de serviços é de sua propriedade e deve ser protegida de riscos e ameaças que possam comprometer sua Confidencialidade, Integridade e Disponibilidade.

Na proteção contra vazamento de informações, utilizamos ferramentas preventivas, instaladas em estações de trabalho, no serviço de correio eletrônico, no serviço de navegação WEB, além de criptografia de disco em notebooks e solução de proteção de dispositivos móveis.

6.15 Proteção dos Dados Pessoais

A proteção dos Dados Pessoais é semelhante à proteção de outros dados e inclui proteger a confidencialidade, integridade e disponibilidade das informações. A Avenue tem os seguintes controles de segurança em vigor para proteger Dados Pessoais:

- Inventário de Dados;
- Proteção dos Dados Pessoais alinhada à matriz de classificação de dados pessoais;
- Controles de acesso ao usuário para Colaboradores individuais e fornecedores terceirizados com acesso aprovado nos termos desta Política;
- Criptografia dos Dados Pessoais; e
- Anonimização dos Dados Pessoais.

Quanto maior o risco e capacidade prejudicial de dano aos clientes e aos titulares dos dados, maior deve ser seu nível de classificação desta informação.

6.16 Gestão da Continuidade dos Negócios

A Avenue mantém processos e procedimentos que garantem a continuidade do seu negócio, utilizando o ambiente de computação em nuvem que permite uma rápida recuperação de seus serviços e produtos, bem como escalabilidade e alta disponibilidade.

6.17 Gestão do Ambiente de Computação em Nuvem

Os ambientes de processamento e armazenamento de dados da Avenue são todos hospedados em ambiente de computação em nuvem que possuem alguns riscos inerentes a este modelo, para isto as seguintes diretrizes devem ser observadas na gestão deste ambiente:

Segurança dos acessos remotos - o acesso seguro para administração e manutenção dos recursos em nuvem devem ser garantidos;

Acesso administrativo - o acesso para administração do ambiente de nuvem é restrito a pessoas autorizadas pela Diretoria da Avenue.

6.18 Backup e Retenção de Dados

A retenção dos dados utilizados na Avenue deve estar de acordo com as regulações aplicáveis tanto no Brasil quanto nos Estados Unidos.

As cópias de backup devem ser armazenadas em local separado do ambiente de produção, com devida proteção contra exclusão e acesso não autorizado.

6.19 Programa de Cybersecurity

O Programa de Cybersecurity da Avenue é norteado pelos seguintes fatores:

- Regulamentações vigentes;
- Melhores práticas;
- Cenários mundiais.

Conforme sua criticidade, o programa divide-se em:

- **Ações críticas:** Consiste em correções emergenciais e imediatas para mitigar riscos iminentes;
- **Ações de Sustentação:** Iniciativas de curto / médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o apetite de risco da Organização e permitindo que ações de longo prazo/estruturantes possam ser realizadas;
- **Ações Estruturantes:** Iniciativas de médio / longo prazo que tratam a causa raiz dos riscos e que preparam a Avenue para o futuro.

O programa de Cybersecurity da Avenue abrange os seguintes componentes:

- Governança, Riscos e Compliance de Cybersecurity;
- Gestão de riscos de terceiros;
- Segurança Corporativa;
    - Arquitetura, engenharia e operações de segurança
    - Métricas de segurança
    - Segurança das aplicações / produtos
    - Testes de invasão

- Operações de segurança:
  - Gestão de vulnerabilidades e patches
  - Inteligência de ameaças
  - Ameaças internas
  - Resposta a incidentes
  - Segurança física

7. Tratamento da Informação

As informações da Avenue e de seus clientes devem ser tratadas de forma ética e sigilosa, utilizadas com transparência e apenas para finalidade definida para a qual foi coletada.

A segregação de funções deve ser observada em todo ciclo de vida da informação de forma a evitar o conflito de interesse.

O acesso às informações e recursos só pode ser realizado mediante autorização (gestão de acesso) e respeitando a diretriz de menor privilégio, na qual os Colaboradores têm acesso somente aos recursos imprescindíveis para o desempenho de suas atividades.

Os colaboradores que manipulam as informações devem ser identificados unicamente e são responsáveis pelas ações realizadas.

Os colaboradores e terceiros são totalmente responsáveis pela correta utilização dos recursos disponibilizados e pelos atos executados com suas senhas, devendo manter sua confidencialidade.

Todos os envolvidos no tratamento da informação da Avenue e de seus clientes devem se comprometer com a confidencialidade assinando um Acordo de Confidencialidade.

8. Privacidade e Direitos de Propriedade

O tratamento da informação deve ser realizado respeitando direitos autorais, regras de licenciamento de softwares, direitos de propriedade, privacidade e proteção de propriedade intelectual.

O tratamento de dados pessoais e dados pessoais sensíveis devem ser realizados em conformidade com a Lei Geral de Proteção de Dados (LGPD).

As diretrizes para o tratamento de dados pessoais na Avenue estão dispostas na Norma de Tratamento de Dados Pessoais.

9. Declaração de Responsabilidade

Os colaboradores, parceiros de negócio e prestadores de serviços da Avenue devem aderir formalmente a um termo, comprometendo-se a agir de acordo com as políticas de Segurança da Informação.

Os contratos firmados com a Avenue devem possuir cláusula que assegure a confidencialidade das informações.

10. Medidas Disciplinares

O descumprimento desta política implicará em advertências formais e dependendo da gravidade e risco poderá resultar no desligamento do colaborador.

11. Definição dos Termos

Ativo de Informação: Qualquer ativo que processe, armazene ou, inclusive, a própria informação

Computação em nuvem: É o fornecimento de serviços de computação, incluindo servidores, armazenamento, bancos de dados, rede, software, análise e inteligência, pela Internet para oferecer inovações mais rápidas, recursos flexíveis e escalabilidade.

Confidencialidade: Garantia de que a informação não estará disponível e nem será divulgada a indivíduos, entidades ou processos sem autorização.

Continuidade do negócio: Capacidade de uma organização de continuar a entrega de produtos e serviços em um nível aceitável após incidentes e interrupções

Dado pessoal: Informação relacionada a pessoa natural identificada ou identificável

Dado pessoal sensível: Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Data Protection Officer (DPO) ou encarregado: Pessoa responsável por atuar como canal de comunicação entre a Avenue, os titulares de dados pessoais e a ANPD

Disponibilidade: Garantia de que os Colaboradores autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Informação: Ativo essencial para o negócio, pode estar na forma escrita, impressa, verbal ou em meio digital ou físico.

Integridade: Corresponde à preservação da precisão, consistência e confiabilidade das informações. Garantia de que a informação não será corrompida, comprometida ou danificada por processamentos sistêmicos, terceiros ou colaboradores.

Violação de dados: Violação de segurança que leva à destruição acidental ou ilícita, à perda, à divulgação não autorizada ou o acesso a dados protegidos e transmitidos, armazenados ou transformados de outro modo.

12. Responsabilidades

12.1 Comitê de Segurança da Informação

- Apoiar e garantir que as políticas e normas sejam cumpridas;
- Garantir que haja um processo educativo e campanhas de sensibilização para promover a cultura de segurança da informação e privacidade.

12.2 Data Protection Officer (“DPO”)

- Receber comunicações da ANPD e adotar as providências internas necessárias para o endereçamento de eventuais solicitações;
- Orientar os Colaboradores a respeito das práticas e procedimentos a serem adotados em relação à proteção de Dados Pessoais;
- Monitorar as estratégias da Avenue com relação à proteção de dados pessoais, por meio de atribuição de responsabilidades, conscientização e treinamento de equipes envolvidas na operação de Tratamento de Dados Pessoais;
- Estabelecer, monitorar e dar a assistência necessária para a criação e efetividade de políticas, procedimentos e medidas de segurança da informação, especialmente aquelas voltadas para a proteção de dados pessoais; e
- Manter registro das operações de Tratamento conduzidas pela Avenue.

12.3 Equipe de Cybersecurity

- Manter esta política sempre atualizada e revisá-la, pelo menos, anualmente;
- Monitorar o ambiente de segurança da informação, a fim de garantir a Confidencialidade, Disponibilidade e Integridade das informações da Avenue e de seus clientes.

12.4 Equipe de Infraestrutura

- Configurar e manter a infraestrutura da Avenue de acordo com as melhores práticas de Segurança da Informação e regulamentações aplicáveis

12.5 Equipe de Compliance

- Garantir a conformidade com esta política.

12.6 Gestores

- Conscientizar os colaboradores sob sua responsabilidade a respeito desta política.

12.7 Colaboradores

- Notificar incidentes de segurança da informação;
- Zelar pela segurança das informações da Avenue e de seus Clientes;
- Cumprir as diretrizes dispostas nesta política.

13. Regulações, Leis e Orientações Externas

Os requisitos desta política devem ser aplicados de acordo com os estatutos, leis, regras, regulamentos e orientações externas das jurisdições em que a companhia opera.

- Resolução CMN No. 4.893 de fevereiro/2021
- Instrução CVM No. 612 de agosto/2021
- Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709/2018
- FINRA Rules
- Norma ABNT ISO/IEC 27001/2022
- Norma ABNT ISO/IEC 27701/2019
- NIST (National Institute of Standards and Technology)

Documento aprovado pela diretoria em 02/02/2024.