1. OBJETIVO

Definir as diretrizes de segurança da informação e privacidade da AGE Desenvolvimento de Sistemas.

2. ABRANGÊNCIA

Todas as unidades de negócios, colaboradores, prestadores de serviços, parceiros e fornecedores da AGE Desenvolvimento de Sistemas.

3. RESPONSÁVEL

A Alta direção da AGE Desenvolvimento de Sistemas é responsável pela viabilização das condições necessárias para a devida aplicabilidade desta Política e a área de Segurança da Informação é responsável pela atualização das Políticas e Normas.

4. TERMOS E DEFINIÇÕES

Vide Manual de Organização de Conceitos

5. DIVULGAÇÃO E DECLARAÇÃO DE RESPONSABILIDADE

A Política deve ser de conhecimento de todos. Sua divulgação e educação são de suma importância para a empresa, e poderá ser divulgada ou publicada das seguintes formas:

a) Impressa;
b) Digital; e
c) Sonora ou Áudio visual.

Cabe as unidades de negócios juntamente com a equipe de segurança da informação e equipe de marketing analisar e definir a melhor forma de divulgação, considerando e respeitando a cultura e costumes, leis e regulamentos vigentes e evitando qualquer tipo de discriminação.

Todos os colaboradores, prestadores de serviços, parceiros e fornecedores que tenham acesso às informações, devem aderir formalmente ao “Termo de Ciência e Recebimento da PSIP”, comprometendo-se a respeitar as Políticas e suas normas de forma integral.

6. PRINCÍPIOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para organização ou seus clientes. Ela pode estar guardada para uso restrito ou exposta ao cliente para consulta ou manuseio.

Entende-se por privacidade o direito da inviolabilidade à intimidade, à vida privada, à honra e a imagem das pessoas.

Todo tipo de ativo de informação é classificado e rotulado, independente da forma apresentada ou o meio do qual a informação é compartilhada ou armazenada. A informação é o maior ativo da AGE Desenvolvimento de Sistemas e de seus clientes, e por isso essencial ao negócio, por esses motivos deverá ser devidamente protegida e utilizada de modo ético e seguro.

Para tanto definimos os pilares de Segurança da informação:

a) **Confidencialidade:** Garantir que a informação não seja revelada ou esteja disponível para indivíduos, entidades e processos não autorizados.
b) **Integridade:** Garantir a salvaguarda da exatidão e totalidade da informação e dos métodos de processamento.
c) **Disponibilidade:** Garantir que a informação esteja sempre acessível e disponível quando necessário. Considerando a:
    1. Prontidão: Ser acessível sempre que necessária,
    2. Continuidade: Manter-se disponível mesmo quando houverem falhas nos sistemas,
    3. Robustez: Atender a todos os usuários do sistema sem que haja uma degradação que comprometa o resultado.
d) **Autenticidade:** Garantir que a autoria seja confirmada.

7. OBJETIVOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

O Sistema Integrado de Gestão de Segurança da Informação e Privacidade (SGSIP) visa preservar a Confidencialidade, Integridade, Disponibilidade e Autenticidade das informações da AGE. Deve estar integrado com os processos da empresa e suas estruturas administrativas.

Os objetivos da segurança da informação e privacidade estão disponiveis no documento P-SGSIP-052 Objetivos Estratégicos da Segurança da Informação.

8. DIRETRIZES DA SEGURANÇA DA INFORMAÇÃO

Para endereçar todo o esforço e manutenção necessária para a Segurança da Informação, a AGE Desenvolvimento de Sistemas estabelece as seguintes diretrizes:

a) Uma estrutura de Gestão da Segurança da Informação e Privacidade foi estabelecida e mantida com apoio da alta direção, através de um Sistema Integrado de Gestão de Segurança da Informação e Privacidade (SGSIP) implementado na AGE;

b) Toda informação deverá ser utilizada com senso de responsabilidade e de modo ético e seguro por todos, em benefício exclusivo dos negócios corporativos, conforme previsto na Norma de conduta ética de colaboradores;
c) A AGE Desenvolvimento de Sistemas reserva-se o direito de monitorar e registrar todo o uso das informações geradas, armazenadas ou veiculadas na empresa. Para tanto foram criados e implantados controles apropriados e trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que a empresa julgou necessário para reduzir os riscos;
d) Todos os ativos de informação estão devidamente identificados, classificados e monitorados;
e) A identificação de cada usuário da AGE Desenvolvimento de Sistemas é única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;
f) Todos os riscos deverão ser analisados, classificados, tratados e apresentados a um Comitê;
g) Todos os incidentes de segurança e violação de dados pessoais são reportados para a área de Segurança da Informação para que sejam analisados, avaliados e tratados pela área responsável.
h) A AGE Desenvolvimento de Sistemas identifica, segue, documenta e mantém atualizadas as leis que regulamentam suas atividades, bem como dos aspectos de propriedade intelectual, conforme apresentado na Declaração de Escopo do SGSIP.
i) A AGE Desenvolvimento de Sistemas, através de sua alta direção definiu os Objetivos Estratégicos de Segurança da Informação e Privacidade considerando esta Política, os requisitos de Segurança da Informação aplicáveis e os resultados da Gestão de Riscos;

9. GESTÃO DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Para manter um nível satisfatório de segurança constitui-se o Comitê de Gestão de Segurança da Informação e Privacidade (CGSIP) que adota Normas, Políticas e outras que possam ser criadas, para sustentar as diretrizes apresentadas:

a) **Norma de Controle de Acesso**: contém a gestão de controle de acesso dos colaboradores internos ou externos, aos ativos de informação que é devidamente aprovado pelo responsável pela informação (gestor, diretoria ou responsável conforme definido nos documentos da informação), a qual o acesso permitirá a manipulação, quer seja para simples consulta ou para alteração;

b) **Norma de Correio Eletrônico**: contém diretrizes organizacionais do e-mail sob "domínio@soc.com.br", permitido apenas para colaboradores internos e externos, e para terceiros somente quando for necessário;

c) **Norma de Cópias de Segurança da Informação (Backup):** contém diretrizes de realização e frequência de Cópias de segurança (backup), através de mídias específicas de informações que são consideradas vitais para o sistema e para a retomada das atividades da área em caso de contingência;

d) **Norma de Desenvolvimento e Projeto Seguro:** contém regras estabelecidas para o desenvolvimento seguro de sistemas e softwares e aplicadas aos desenvolvimentos realizados dentro da organização;

e) **Norma de Classificação e Manuseio da Informação**: contém diretrizes para classificação, rotulagem e demais regras para manuseio das informações de acordo com a confidencialidade e as proteções necessárias, da seguinte forma: Pública, Sensível, Privada e Confidencial, classificando, quando houver, dados pessoais ou dados pessoais sensíveis, e devem ser tratadas, armazenadas e descartadas de maneira correta para garantir os aspectos de segurança da informação e privacidade no negócio da AGE e nas informações dos seus clientes;

f) **Norma de Conduta Ética de Colaboradores:** contém diretrizes e regras sobre as responsabilidades de colaboradores quanto a segurança da informação, seguindo requisitos mínimos de conduta e ética estão definidas;

g) **Norma de Gestão de Ativos:** A AGE possui processos mapeados, além dos ativos tangíveis e intangíveis de informação identificados de forma individual, inventariados, protegidos e monitorados de acessos indevidos. As mídias são gerenciadas de forma adequada, conforme os requisitos de segurança da informação estabelecidos e implementados;

h) **Norma de Gerenciamento de Chaves Criptográficas e Transmissão de Informações:** contendo diretrizes que estabelecem um conjunto de regras adotadas para garantir a padronização das técnicas criptográficas, a aplicação adequada delas e responsabilidades, visando manter a segurança no transporte ou armazenamento das informações, independentemente do meio utilizado. Contém ainda regras quanto à transmissão de

informações, para os recursos, prevendo a utilização do controle inclusive para dados pessoais tratados pela organização a fim de garantir a privacidade na comunicação dos dados da AGE Desenvolvimento de Sistemas e de seus clientes;

i) **Norma de Gerenciamento de Mudanças**: Um processo de gestão de mudanças está em vigor para garantir que controles e modificações nos sistemas ou recursos de processamento da informação sejam realizados com planejamento, a fim de não ocasionar falhas operacionais ou de segurança no ambiente produtivo da organização;

j) **Norma de Mesa Limpa e Tela Protegida**: contém diretrizes para a proteção das informações reduzindo os riscos de acesso não autorizado, perda ou dano à informação durante e fora do horário normal de trabalho, foram adotadas medidas de segurança;

k) **Norma de Análise, Avaliação e Tratamento de Riscos:** contendo diretrizes e regras para identificação dos riscos por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os processos nos aspectos de segurança da informação;

l) **Norma de Gestão de Incidentes de Segurança da Informação:** contendo diretrizes para a gestão de todos os incidentes que afetem a segurança da informação e violação de dados pessoais, sendo reportado via processo, canal seguranca@soc.com.br ou telefone, sendo encaminhado para área de Segurança da Informação que analisa o incidente e toma as ações devidas, repassando a tratativa as áreas responsáveis;

m) **Norma de Tecnologia da Informação e Uso aceitável de Ativos:** Estão regulamentadas as responsabilidades de Tecnologia da Informação e restrições do uso de ativos na organização;

n) **Norma de Indicadores e Métricas do SGSIP**: contendo diretrizes para garantir a melhoria contínua do Sistema Integrado de Gestão da Segurança da Informação e Privacidade (SGSIP), com base na norma ISO/IEC 27001:2022e ISO/IEC 27701:2019, contendo os indicadores e métricas para monitoramento do SGSIP durante todo o ciclo PDCA;

o) **Norma de Conformidade**: Define regras para garantir que não ocorram violações juridicas, regulamentares ou contratuais nos requisitos de segurança da informação na organização;

p) **Norma de Segurança Física e Ambiente:** contém diretrizes para que o acesso físico às instalações onde os ativos de TI e informações criticas à continuidade do negócio, sejam controlados de forma a garantir a sua proteção, disponibilidade, integridade e confidencialidade;

q) **Norma de Conduta Ética de Fornecedores:** contém diretrizes que visam garantir que não ocorram violações jurídicas, regulamentares ou contratuais nos requisitos de segurança da informação na organização em relação ao gerenciamento de serviços realizados por fornecedores, parceiros e terceiros, utilizando de uma postura ética compatível com os princípios, valores da AGE e promovam uma relação mais justa e sustentável;

r) **Política de Proteção de Dados Pessoais:** contém diretrizes que visam garantir a gestão sistemática e efetiva dos aspectos relacionados à proteção de dados pessoais e dos direitos dos seus titulares, atendendo a leis de privacidade de dados.

Quando razões tecnológicas ou determinações superiores tornarem impossível a aplicação dos requisitos previstos nesta política, o responsável e/ou solicitante deverá documentá-las imediatamente à área de Segurança da Informação ou área responsável para que possibilite a adoção de medidas alternativas que minimizem os riscos, bem como um plano de ação para corrigi-los, monitorá-los ou eliminá-los.

10. MONITORAMENTO E AUDITORIA

A AGE Desenvolvimento de Sistemas monitora e registra todo o uso das informações geradas, armazenadas ou veiculadas na empresa. Para tanto a organização mantém controles apropriados e trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que a empresa julgou necessário para reduzir os riscos, e reservar-se o direito de:

a) Implantar outros sistemas de monitoramento de acesso às estações de trabalho, servidores internos e externos, correio eletrônico, navegação, Internet, dispositivos móveis ou *wireless* e outros componentes da rede. A informação gerada por estes sistemas de monitoramento poderá ser usada para identificar usuários e respectivos acessos efetuados;

b) Inspecionar qualquer arquivo que esteja na rede, no disco local da estação ou qualquer outro ambiente, visando assegurar o rígido cumprimento desta PSIP;

c) Instalar outros sistemas de proteção e detecção de invasão para garantir a segurança das informações e dos perímetros de acesso.

11. PENALIDADES

Para toda e qualquer infração à política e demais Normas de Segurança da Informação e Privacidade deve ser aberto um incidente de segurança da informação, que será analisado e tratado de acordo com a Norma de Gestão de Incidentes de Segurança da Informação e, por conseguinte, apurada através de procedimentos internos, que devem ser conduzidos pelo responsável da área em que se encontra alocado o profissional que cometeu a infração, em conjunto com a área de Desenvolvimento Humano Organizacional (DHO).

Caso o CGSIP julgue cabível, o colaborador envolvido poderá, enquanto durar o processo de apuração interna, ser afastado da função ou suspenso.

Ao colaborador suspeito de cometer violações à Política e Normas de Segurança da Informação, deverá ser assegurado tratamento justo e correto, sendo que toda e qualquer medida resultante de sua infração deverá ser aplicada com proporcionalidade à ocorrência com base no Código de Conduta, Termo de Confidencialidade, Manual do Colaborador e Processo Disciplinar da AGE Desenvolvimento de Sistemas e legislações vigentes.

A AGE Desenvolvimento de Sistemas exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, terceiros e parceiros, reservando-se o direito de punir os infratores, analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios e adotar as medidas legais cabíveis.

12.ESCOPO DE CERTIFICAÇÃO DO SGSIP

O escopo contemplado no Sistema Integrado de Gestão de Segurança da Informação e Privacidade (SGSIP) está descrito no certificado ISO 27.001 e no documento de Declaração de escopo.

13. ANEXO 1 - TERMO DE CIÊNCIA E RECEBIMENTO DA PSIP

Dados do Usuário	
Nome Completo:	
Área / Depto:	Localidade:
Empresa (caso não funcionário):	
CNPJ (caso não funcionário):	
Prazo de Acesso: ☐ Indeterminado	☐ Temporário até ____/____/____

• Informo para devidos fins que li e entendi o documento chamado “P-SGSIP-001 Política de Segurança da Informação e Privacidade”.

• Por meio da assinatura desse termo, manifesto minha concordância em todos os itens descritos neste documento e as Normas a ele atreladas e me comprometo em segui-los.

• Comprometo-me também em sempre estar atento ás atualizações das Políticas e Normas.

• Este documento deverá ficar guardado junto ao prontuário do colaborador pela área de Desenvolvimento Humano Organizacional (DHO).

_____ _____

Local e Data Assinatura