1. OBJETIVO

Definir as diretrizes de segurança da informação 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 PSI e a Coordenadoria de Segurança da Informação é responsável pela atualização dessa Política.

4. TERMOS E DEFINIÇÕES

Vide Manual de Organização de Conceitos

5. DIVULGAÇÃO E DECLARAÇÃO DE RESPONSABILIDADE

A PSI 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 e divulgação 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 tenha acesso a informações, devem aderir formalmente ao “Termo de Ciência e Recebimento da PSI”, comprometendo-se a respeitar esta PSI e suas normas de forma integral.

6. PRINCÍPIOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

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.

Todo tipo de ativo de informação é classificado, podendo ser rotulado como: Confidencial, Privado, Sensível ou Público. 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.

7. OBJETIVOS DE SEGURANÇA DA INFORMAÇÃO

O Sistema de Gestão de Segurança da Informação (SGSI) estabelecido na AGE Desenvolvimento de Sistemas, visando manter a Segurança da Informação (SI) nos pilares de confidencialidade, integridade e disponibilidade tem como premissa as seguintes ações:

- Assegurar que a Informação seja protegida contra acesso indevido, mantendo a confidencialidade, integridade e disponibilidade;
- Garantir que os ativos de processamento de informação sejam corretamente controlados;
- Definir e testar planos de recuperação de desastres, de forma a reestabelecer os serviços restados no menor tempo possível;
- Realizar atividades de conscientização com todos os envolvidos do Sistema de Gestão de Segurança da Informação (SGSI), declarando as responsabilidades.

Todas a ações definidas são monitoradas e controladas por meio de indicadores apresentados para Alta Direção.

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.

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 será estabelecida e mantida com apoio da alta direção, através de um Sistema de Gestão de Segurança da Informação (SGSI);

b) A informação deverá ser utilizada com senso de responsabilidade e de modo ético e seguro por todos, em benefício exclusivo dos negócios corporativos;

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 colaborador 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 e apresentados a um Comitê que deliberará sobre o Tratamento adequado para tais;

g) Todos os incidentes de segurança devem ser reportados para o Departamento de Segurança da Informação para que sejam analisados, avaliados e tratados pela area responsável.

h) A AGE Desenvolvimento de Sistemas identifica, segue, documenta e mantem atualizadas as leis que regulamentam suas atividades, bem como dos aspectos de propriedade intelectual.

i) A AGE Desenvolvimento de Sistemas, através de sua alta direção definiu os Objetivos Estratégicos de Segurança da Informação considerando esta Política, os requisitos de Segurança da Informação aplicáveis e os resultados da Gestão de Riscos.

9. GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Para manter um nível satisfatório de segurança constitui-se o Comitê de Gestão de Segurança da Informação (CGSI) que adotará as seguintes normas, e outras que possam ser criadas, para sustentar as diretrizes apresentadas:

a) Norma de Controle de Acesso: O controle de acesso dos colaboradores internos ou externos aos ativos de informação deve ser devidamente aprovado pelo responsável pela informação (gestor, diretoria ou responsavel 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: O uso do e-mail sob domínio@soc.com.br, será permitido para colaboradores internos e externos, e para terceiros somente quando for necessário, e por tempo determinado pela gerência da área solicitante mediante a Termo de responsabilidade. Este tempo poderá ser prorrogado mediante nova solicitação da gerência da área.

c) Norma de Cópias de Segurança da Informação (Backup): 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 Seguro: Regras para o desenvolvimento seguro de sistemas e softwares estão estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização;

e) Norma de Acesso Remoto: Concessão de acesso remoto para os colaboradores internos ou externos deve ser autorizada formalmente e solicitada à área de Tecnologia da Informação e operações pelo gestor da área, ocasião em que deverá ser indicado o tipo de acesso, permissão e as informações a serem acessadas;

f) Norma de Dispositivos Móveis: Dispositivo móvel entende-se qualquer equipamento eletrônico com atribuições de mobilidade no manuseio da informação e destina-se ao uso em serviço para realização de suas atividades de trabalho e para comunicação com a empresa, fornecedores ou clientes, devendo ser utilizado somente para esta finalidade;

g) Norma de Classificação e Manuseio da Informação: As informações devem ser classificadas e manuseadas de acordo com a confidencialidade e as proteções necessárias, da seguinte forma: Pública, Sensível, Privada e Confidencial, e devem ser tratadas, armazenadas e descartadas de maneira correta para garantir os aspectos de segurança da informação no negócio da AGE e nas informações dos seus clientes;

h) Norma de Conduta Ética de Colaboradores: As responsabilidades de todos quanto a segurança da informação, seguindo requisitos mínimos de conduta e ética estão definidas;

i) Norma de Gestão de Ativos: Os ativos tangíveis e intangíveis de informação estão identificados de forma individual, inventariados, protegidos e monitorados de acessos indevidos. E mídias são gerenciadas de forma adequada, conforme os requisitos de segurança da informação;

j) Norma de Gerenciamento de Chaves Criptográficas e Transmissão de Informações: Um conjunto de regras para garantir a padronização das técnicas criptográficas, a aplicação adequada das mesmas e responsabilidades para manter a segurança no transporte ou armazenamento das informações independente do meio utilizado. Quanto à transmissão de informações, este recurso é utilizado para garantir a privacidade na comunicação dos dados da AGE Desenvolvimento de Sistemas e de seus clientes;

k) Norma de Gerenciamento de Mudanças de TI: 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, afim de não ocasionar falhas operacionais ou de segurança no ambiente produtivo da organização;

l) Norma de Mesa Limpa e Tela Protegida: Para garantir a proteção das informações de maneira eficaz e reduzir os riscos de acesso não autorizado, perda ou dano à informação durante e fora do horário normal de trabalho, foram adotadas medidas de segurança;

m) Norma de Análise, Avaliação e Tratamento de Riscos: Os riscos são identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os processos nos aspectos de segurança da informação (Confidencialidade, Integridade e Disponibilidade);

n) Norma de Gestão de Incidentes de Segurança da Informação: Todos os incidentes que afetem a segurança da informação devem ser reportados ao Departamento de Segurança da Informação através do canal seguranca@soc.com.br, que analisará o incidente e tomará as ações devidas, repassando a tratativa as áreas responsáveis;

o) 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;

p) Norma de Indicadores e Métricas do SGSI: Para garantir a melhoria contínua do Sistema de Gestão da Segurança da Informação (SGSI), com base na norma ISO/IEC 27001:2013, contém todos os indicadores e métricas para monitorar-se o ciclo PDCA;

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

r) Norma de Segurança Física e Ambiente: Para garantir que o acesso físico às instalaçoes onde os ativos de TI e informações criticas à continuidade do negocio estejam armazenados sejam controlados de forma a garantir a sua proteção, disponibilidade, integridade e confidencialidade.

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 por, 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 mantem 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 eletrônicos, 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 PSI;

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 PSI e às Normas de Segurança da Informação deverá ser aberto um incidentes de segurança da informação, tratado de acordo com a norma de Gestão de Incidentes de Segurança da Informação e informado ao CGSI e, por conseguinte, apurada através de procedimentos internos, que deve ser conduzido pelo gestor da área em que se encontra alocado o profissional que cometeu a infração, em conjunto com o Departamento de Recursos Humanos e o Jurídico da AGE Desenvolvimento de Sistemas.

Caso o CGSI 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 Codigo de Conduta, Termo de Confidencialidade, Manual do Colaborador 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, 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. DECLARAÇÃO DE ESCOPO

A AGE Desenvolvimento de Sistemas está comprometida em promover uma gestão sistemática de Segurança da Informação que garanta a proteção de seus processos, ativos de informação, e informações de seus clientes.

Para atingir este objetivo, a AGE Desenvolvimento de Sistemas implementou um Sistema de Gestão de Segurança da Informação (SGSI) em conformidade com a norma ISO/IEC 27001:2013.

12.1 Escopo para certificação

O escopo do Sistema de Gestão de Segurança da Informação (SGSI) contempla os processos de Desenvolvimento, Serviços e Tecnologia da Informação para a ferramenta SOC.

Estes processos são executados no seguinte local:

Endereço do Escritório: Avenida Ana Costa, 255, conj 41, 42, mezanino e 10 andar em Santos/SP