Política de Segurança da Informação e Privacidade - PSIP AFEAM

AFEAM
Agência de Fomento do Estado do Amazonas S.A.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Introdução

A Agência de Fomento do Estado do Amazonas S/A – AFEAM é uma empresa pública, classificada como instituição financeira não bancária, subordinada à fiscalização e supervisão do Banco Central do Brasil e organizada sob forma de sociedade anônima, de capital fechado.

Plenamente integrada à sociedade digital, a AFEAM tem, entre seus ativos, todo conhecimento acumulado, métodos e estratégias desenvolvidas ao longo da sua história, os dados que compila, estuda e disponibiliza, além de sua imagem e reputação frente ao apoio financeiro, creditício e técnico às iniciativas que estimulam o desenvolvimento dos setores produtivos da economia amazonense.

São esses ativos que garantem a importância da AFEAM no mercado, e que devem ser adequadamente manuseados e protegidos por todos os seus colaboradores, por meio da adoção de uma Política de Segurança da Informação e Privacidade, capaz de normatizar e alinhar as condutas esperadas pela Instituição.

Este documento depende da combinação de requisitos do negócio, de estrutura de processos, do uso de tecnologias e mecanismos de proteção e, o mais relevante, o comportamento de seus colaboradores, independentemente do nível hierárquico ou da atividade desenvolvida para a AFEAM.

Para ampliar a cultura de segurança da informação e privacidade, a AFEAM alinhada as boas práticas e normas internacionalmente aceitas, atualizou esta política, a fim de adequá-la à legislação nacional vigente para garantir a proteção de dados pessoais e de todos os seus ativos tangíveis e intangíveis.

1. Objetivos

1.1 Declarar formalmente, por meio de seus Administradores, as diretrizes da AFEAM que visam à proteção dos ativos de informação com eficiência, eficácia e competitividade, de modo seguro, garantindo a confidencialidade, integridade, disponibilidade, autenticidade e legalidade, assim como dos ativos de tecnologia de informação que as sustentam, de forma alinhada aos requisitos legais e exigências dos órgãos regulatórios de acordo com o negócio;

1.2 Esclarecer as responsabilidades de todos os envolvidos direta ou indiretamente com os dados pessoais e as informações da AFEAM, bem como as diretrizes a serem consideradas para preservar, proteger e assegurar a privacidade destes dados, e os recursos que processam e/ou transportam estas informações;

1.3 Prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético da AFEAM.

2. Aplicação

2.1 A Política de Segurança da Informação e Privacidade é um documento interno, com valor jurídico e aplicabilidade imediata, plena e indistinta.

2.2 Para efeito desta política:

2.2.1 Administradores – membros do Conselho de Administração e Diretoria Colegiada;

2.2.2 Órgãos Estatutários – membros do Conselho de Fiscal e do Comitê de Auditoria;

2.2.3 Empregados Públicos – pessoas com vínculo empregatício com a AFEAM pertencentes ao quadro de efetivos e não efetivos;

2.2.4 Colaboradores – estagiários, aprendizes, terceirizados, parceiros técnicos e representantes de órgãos de regulação e controle e auditores externos no exercício de suas atividades nas dependências da AFEAM;

2.2.5 Outros – fornecedores, clientes e todo agente que, por força de lei, contrato ou de qualquer ato jurídico, preste serviço à AFEAM de natureza permanente, temporária ou excepcional, ainda que sem retribuição financeira.

3. Diretrizes Gerais

3.1 Assegurar o cumprimento de todas as suas obrigações legais, para atender aos requisitos regulamentares e contratuais pertinentes às suas atividades, a exemplo da Lei Geral de Proteção de Dados Pessoais - LGPD, n° 13.709/2018 e da Resolução nº 4893/2021 do BACEN;

3.2 Empregar medidas técnicas e organizacionais adequadas no tratamento de dados pessoais, e envidar esforços para proteção dos dados pessoais dos titulares contra acessos não autorizados, perda, destruição, compartilhamento não autorizado, entre outras hipóteses;

3.3 Garantir a confidencialidade, integridade e disponibilidade das informações da própria AFEAM, protegendo os sistemas de informação contra acessos indevidos e modificações não autorizadas;

3.4 Assegurar que somente pessoas autorizadas tenham acesso às instalações, às informações e aos sistemas de informação da AFEAM;

3.5 Conscientizar as pessoas das possíveis consequências para a AFEAM e para os seus usuários, sobre incidentes de segurança da informação ou violação às Políticas de Segurança, Privacidade e Cibersegurança;

3.6 Garantir a continuidade de seus negócios, protegendo os processos críticos contra falhas ou desastres significativos;

3.7 Assegurar o treinamento contínuo e atualizado nas políticas e nos procedimentos de Segurança da Informação e Privacidade, enfatizando as obrigações das pessoas pela proteção de dados;

3.8 Garantir que todas as responsabilidades pela Segurança da Informação e Privacidade, estejam claramente definidas e que as pessoas indicadas são competentes e capazes de cumprir com as atribuições;

3.9 Melhorar continuamente o Programa de Segurança da Informação e Privacidade.

4. Controles Gerais

4.1 Interpretação: Esta PSIP e seus documentos complementares devem ser interpretados de forma restritiva, dentro do princípio de aplicação do menor privilégio possível, ou seja, tudo o que não estiver expressamente permitido só deve ser realizado após autorização do Comitê de Segurança da Informação e Privacidade - CSIP, devendo ser levada em consideração a análise de risco (GECOR) e a necessidade do negócio à época de sua solicitação;

4.2 Publicidade: Esta PSIP e seus documentos complementares devem ser divulgados aos Administradores, Membros dos Órgãos Estatutários, Empregados e Colaboradores, visando a sua disponibilidade para todos que se relacionam com a AFEAM, ou que, direta ou indiretamente, são impactados;

4.3 Propriedade: As informações geradas, produzidas, acessadas, manuseadas, armazenadas ou descartadas no exercício das atividades realizadas pelos Administradores, Membros dos Órgãos Estatutários, Empregados e Colaboradores, bem como os demais ativos intangíveis e tangíveis disponibilizados, são de propriedade e direito de uso exclusivo da AFEAM e devem ser empregados unicamente para fins profissionais, não cabendo qualquer forma de direito autoral;

4.4 Classificação da Informação: Os Administradores, Membros dos Órgãos Estatutários, Empregados e Colaboradores devem utilizar apenas os recursos disponibilizados pela AFEAM para classificar a informação e aplicar os respectivos controles estabelecidos em documento específico, em todo o ciclo de vida da informação, ou seja, desde a sua recepção ou produção até o seu descarte;

4.5 Sigilo: É vedada a revelação de qualquer informação de propriedade ou sob a responsabilidade da AFEAM, por seus Administradores, Membros dos Órgãos Estatutários, Empregados e Colaboradores, sem a prévia e formal autorização para tanto, inclusive no âmbito acadêmico, excetuando-se a hipótese de que a informação esteja classificada como “pública”;

4.5.1 A AFEAM não autoriza a utilização dos meios de comunicação da organização para divulgar mensagens com conteúdo ilegal, pornográfico, com qualquer sentido discriminatório, de cunho religioso, político-partidário, ideológico ou em desacordo com os princípios éticos e morais;

4.6 Uso dos Ativos de Tecnologia da Informação: Os ativos de informação de propriedade da AFEAM devem ser utilizados apenas para fins profissionais, de modo lícito, ético, moral e aprovado administrativamente.

4.6.1 Os Administradores, Membros dos Órgãos Estatutários, Empregados e Colaboradores devem utilizar apenas ativos de informação previamente homologados e autorizados pela Gerência de Tecnologia da Informação - GETI sejam eles onerosos, gratuitos, livres ou licenciados;

4.6.2 Internet: A Internet é uma ferramenta de trabalho para o desenvolvimento de atividades, processos, pesquisas, tecnologias e competências. A AFEAM mantém regras de utilização e bloqueio de acesso a determinados sites, caixas de e-mail, conteúdos, anexos, emitentes, destinatários, assinaturas, notas, limites de tráfego e armazenamentos.

4.7 Autenticação: Os Administradores, Membros dos Órgãos Estatutários, Empregados e Colaboradores são responsáveis pelo uso e sigilo de suas credenciais de acesso, onde não é permitido, em qualquer hipótese, compartilhar, revelar ou fazer uso não autorizado de credenciais de terceiros, sendo responsável direto pela conduta ou/e dano causado, mediante apuração de responsabilidade em Processo Administrativo Disciplinar devidamente instaurado;

4.8 Sistema Operacional para a implantação de ferramentas de criptografia, além de garantir o seu uso efetivo e adequado, com o intuito de garantir a segurança das informações na AFEAM;

4.9 Prevenção e Detecção de Intrusão: A AFEAM possui ferramentas para realizar monitoramento e análise de eventos em sistemas computacionais, com o propósito de detectar e prover alertas sobre tentativas de acesso não autorizado a recursos destes sistemas;

4.10 Prevenção de vazamento de informações: Arquivos contendo dados sensíveis da AFEAM, quando transferidos de qualquer forma pela internet, devem estar protegidos de vazamento, adulteração e outras ameaças à integridade e confidencialidade da informação;

4.11 Proteção contra softwares maliciosos: A AFEAM possui um pacote de software de segurança, que consiste em recursos antimalware, prevenção de intrusões e firewall para servidores e computadores desktop;

4.12 Realização periódica de testes e varreduras para detecção de vulnerabilidades: Serão realizadas varreduras de vulnerabilidade e testes de intrusão ao menos 2 (duas) vezes por ano;

4.13 Estabelecimento de mecanismos de rastreabilidade: O uso dos recursos de tecnologia da informação e comunicações disponibilizados pela AFEAM é passível de

monitoramento, rastreio e auditoria, devendo ser implementados e mantidos, à medida do possível, mecanismos que permitam a sua rastreabilidade, através da utilização de solução DLP;

4.14 Segmentação da rede de computadores: Por questões de segurança e preservação de desempenho, a infraestrutura de rede da AFEAM está segmentada. Cabe a Gerência da Tecnologia da Informação - GETI avaliar e propor segmentação da rede corporativa, de acordo com o perfil e necessidade dos usuários;

4.15 Controle de acesso: A AFEAM controla o acesso físico e lógico às suas dependências e aos seus ativos de informação, contudo toda aplicação/sistema de uso da empresa deve possuir forma de controle e acesso. Desse modo, os Administradores, Membros dos Órgãos Estatutários, Empregados e Colaboradores devem possuir uma credencial de acesso de uso individual, intransferível e, sempre que aplicável, de conhecimento exclusivo;

4.16 Salvaguarda (backup): A AFEAM deve definir e manter um processo de salvaguarda e restauração das informações e de seus ativos de informação críticos, a fim de atender aos requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas ou incidentes;

4.17 Desenvolvimento seguro e aquisição de software: O desenvolvimento interno e/ou externo de softwares, assim como a aquisição de softwares e produtos no mercado, devem possuir requisitos de segurança para garantir informações confiáveis, íntegras, autênticas e oportunas;

4.18 Segurança em Ambiente para Computação em Nuvem (Cloud Computing): a AFEAM é responsável pela confiabilidade, integridade, disponibilidade, segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor;

4.19 Gerenciamento de Riscos Cibernéticos: A AFEAM deve analisar, em intervalos regulares, seus processos e ativos de informação, visando assegurar que estes estejam devidamente mapeados, inventariados e com seus gestores identificados e cientes, assim como suas vulnerabilidades e ameaças de segurança identificadas;

4.20 Manutenção dos Ativos de informação: Todos os ativos de informação em uso no ambiente corporativo da AFEAM devem atender as recomendações de seus fabricantes ou desenvolvedores, no que diz respeito à manutenção, atualizações e correções de falhas técnicas de segurança;

4.21 Mobilidade: Os ativos de informação que permitem mais mobilidade aos Administradores, Membros dos Órgãos Estatutários, Empregados devem ser utilizados somente quando fornecidos ou autorizados pela AFEAM, que deve ocorrer somente após solicitação formal e fundamentada do solicitante e autorização expressa, quando for o caso do Gestor da unidade e da GETI. Além disso, devem estar diretamente relacionados a uma justificativa do negócio, com motivo estritamente profissional;

4.21.1 As diretrizes gerais de uso de dispositivos móveis para acesso às informações, sistemas, aplicações e e-mail da AFEAM devem considerar, prioritariamente, os

requisitos legais e a estrutura da organização, atendendo a esta Política de Segurança da Informação e a Política de Proteção de Dados, e devem ser regidas por normas específicas, a qual contempla as recomendações sobre o uso desses dispositivos.

4.22 Ativos de informação Particulares: O uso de ativos de informação particulares na execução de qualquer atividade profissional ou na interação com os ambientes físicos ou lógicos ou com as informações da AFEAM deve ocorrer somente após solicitação formal e fundamentada dos Administradores, Empregados solicitantes e autorização expressa, quando for o caso do Gestor da unidade e da GECOR e GETI;

4.23 Repositórios digitais: É vedado aos Administradores, Membros dos Órgãos Estatutários, Empregados e Colaboradores o uso de repositórios digitais particulares (ex: dropbox, iCloud, WeTransfer, Google Drive e outros), nos ativos de informação da AFEAM, salvo casos onde seja realizada solicitação formal e aprovada pelo CSIP;

4.24 Softwares de comunicação instantânea: É vedado aos Administradores, Empregados e Colaboradores a instalação e o uso de softwares de comunicação instantânea não homologados pela GETI nos ativos de informação da AFEAM, salvo casos onde seja realizada solicitação formal e aprovada pelo CSIP;

4.25 Mídias Sociais: A participação dos Administradores, Membros dos Órgãos Estatutários, Empregados e Colaboradores nas mídias sociais por meio dos ativos de informação da AFEAM deve ser realizada de acordo com o item Participação em Redes Sociais e outras mídias do Código de Ética, Conduta e Integridade da AFEAM e da Política e Procedimento de Divulgação de Informações da AFEAM.

4.25.1 Os Administradores, Membros dos Órgãos Estatutários, Empregados e Colaboradores são responsáveis por sua conduta no uso das mídias sociais. Por isso, cuidados devem ser tomados em relação ao excesso de exposição (rotinas, trajetos, intimidade etc.), no uso de conteúdos autorizados e legítimos e na preservação do sigilo profissional;

4.25.2 A utilização de perfis institucionais mantidos em redes sociais com o objetivo de prestar atendimento e serviços, divulgando ou compartilhando informações da AFEAM, com autorização previamente constituída pelas áreas de gestão, deve ser regida pelo Código de Ética, Conduta e Integridade e pela Política e Procedimentos de Divulgação de Informações da AFEAM devendo estar em consonância tanto com esta PSIP quanto com os objetivos estratégicos da organização. Para Informações adicionais consulte a norma.

4.26 Ambientes Lógicos: Os sistemas e processos que suportam os ativos de informação da AFEAM devem ser confiáveis, íntegros e disponíveis, a quem deles necessite para execução de suas atividades profissionais;

4.27 Ambientes Físicos: A AFEAM deve estabelecer perímetros de segurança para proteção de suas propriedades, bem como implementar controles de identificação e registro de acesso em todas suas dependências;

4.28 Áudio, Vídeos e Fotos: É vedada qualquer atividade relacionada à gravação de áudio,

vídeo ou foto sobre informações classificadas como restrita ou confidencial dentro das dependências da AFEAM;

4.29 Prestação de Serviços: Os relacionamentos e contratações, inclusive de colaboradores, em que ocorra o compartilhamento de informações da AFEAM ou a concessão de qualquer tipo de acesso aos seus ambientes e ativos de informação, devem ser precedidos por termos de confidencialidade e cláusulas contratuais relacionadas à Segurança da Informação e Privacidade. A PSIP FORNECEDOR é a Política de Segurança da Informação e Privacidade própria para prestadores de serviços e fornecedores.

4.30 Documentação: A AFEAM deve possuir documentação adequada e suficiente para garantir a compreensão e rápida recuperação em situações de contingência de seus sistemas e processos que envolvam seus ativos de informação crítico;

4.31 Monitoramento: A AFEAM realiza o monitoramento, inclusive de forma remota, de todo acesso e uso de suas informações, ativos de informação e seus ambientes físicos e lógicos, visando a eficácia dos controles implantados, a proteção de seu patrimônio e sua reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes referente a segurança da informação;

4.32 Gestão de Configuração e Mudança: O andamento e o resultado de uma mudança, principalmente nos sistemas e infraestrutura tecnológica da AFEAM devem preservar os controles relacionados a disponibilidade, integridade, sigilo e autenticidade das informações;

4.33 Continuidade do Negócio: No escopo das ações de Segurança da Informação e Privacidade, os procedimentos de Gestão da Continuidade de Negócios devem ser executados em conformidade com os requisitos de segurança estabelecidos para proteção dos ativos de informação críticos. O plano deve ser aprovado pela Diretoria Colegiada da AFEAM e validado periodicamente por meio de simulações e os resultados dos testes devem ser documentados.

4.34 Em nenhum caso, Administradores, Membros dos Órgãos Estatutários, Empregados e Colaboradores poderão compartilhar ou transferir informações da AFEAM ou de responsabilidade desta a terceiros, ou fornecer acesso a elas sem a autorização formal e prévia.

4.35 Capacitação: A AFEAM deve desenvolver um Programa Anual de Conscientização em Segurança da Informação e Cibersegurança para capacitação, avaliação e disseminação da cultura de Segurança da Informação e Privacidade junto aos Administradores, Membros dos Órgãos Estatutários, Empregados e Colaboradores;

4.36 Investimentos: Os investimentos em Segurança da Informação e Privacidade na AFEAM devem ser estudados e deliberados conjuntamente com o CSIP, considerando a viabilidade dos investimentos (custo x benefício) e os impactos de sua aplicação à qualidade dos processos de negócio;

4.37 Comitê de Segurança da Informação e Privacidade: A AFEAM deve manter um Comitê de Segurança da Informação e Privacidade - CSIP, com composição fixa de

representantes da GETI, GETEC, GECOB, GECAT, GECOR, GERAD, GEJURI e GEPEC e Responsável pela Segurança da Informação e Privacidade, cuja principal função está em assessorar a implementação das ações relacionadas à segurança da informação e privacidade, além de avaliar os controles e incidentes relacionados. O Comitê se reunirá, ordinariamente a cada 3 (três) meses e, extraordinariamente, quando convocado por algum de seus membros;

4.38 Equipe de Resposta a Incidentes: A AFEAM deve manter uma equipe de resposta a incidentes em segurança da informação e privacidade, preparada para receber, registrar, analisar a causa e impacto (abrange inclusive informações recebidas de empresas prestadoras de serviços a terceiros), responder a notificações e atividades relacionadas a incidentes de segurança da informação e privacidade, bem como o controle dos efeitos de incidentes relevantes para as atividades da AFEAM. Elaborar e testar cenários de incidentes considerados nos testes de continuidade de negócio. Essa equipe deverá estar subordinada ao CSIP;

4.39 Comunicação de Incidentes: A AFEAM deve possuir um canal de comunicação divulgado aos Administradores, Membros dos Órgãos Estatutários, Empregados e Colaboradores para reportar imediatamente os possíveis casos de incidentes de segurança da informação e privacidade, podendo fazer de modo formal ou com uso do recurso de denúncia anônima;

4.39.1 Será realizada a comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes que configurem uma situação de crise pela AFEAM, bem como das providências para o reinício das suas atividades.

4.40 Exceções: As exceções que ocorram de forma exclusiva e excepcional a essa PSIC, devem ser formalizadas e fundamentadas pelos Administradores, Membros dos Órgãos Estatutários, Empregados e Colaboradores solicitantes, e podem ser revogadas a qualquer tempo, por mera liberalidade do CSIP, conforme previsto em procedimento específico.

4.41 Dúvidas: Qualquer dúvida relativa a esta PSIP deve ser encaminhada ao CSIP por meio do e-mail csip@afeam.org.br.

5. Papéis e Responsabilidades

5.1 Conselho de Administração

5.1.1 Aprovar a implantação, ajustes e atualizações com base em Parecer proposto pelo Comitê de Segurança da Informação e Privacidade - CSIP.

5.2 Diretor responsável pela Segurança da Informação e Privacidade

5.2.1 Diretor Administrativo responsável por manter a eficiência e eficácia da Segurança da Informação e Privacidade da AFEAM.

5.3 Diretoria Colegiada

5.3.1 Aprovar sobre o planejamento das atividades relacionadas à Gestão de Segurança da Informação e Privacidade;

5.3.2 Deliberar sobre a implantação/alteração de Políticas, Normas e Procedimentos e demais proposições relacionadas à Política de Segurança da Informação e Privacidade propostas pela GECOR, com base no Parecer emitido pelo CSIP;

5.3.3 Deliberar sobre resultado de auditoria interna relacionada à Segurança da Informação e Privacidade apresentado pela Auditória Interna - AUDIN;

5.3.4 Deliberar sobre o Relatório de Posição das Atividades relacionadas à Gestão de Segurança da Informação e Privacidade elaborado pelo Responsável pela Segurança da Informação e Privacidade;

5.4 Comitê de Segurança da Informação e Privacidade – CSIP

5.4.1 Analisar e emitir Parecer para a Diretoria Colegiada sobre o planejamento das atividades relacionadas à Gestão de Segurança da Informação e Privacidade, encaminhado pelo Responsável pela Segurança da Informação e Privacidade;

5.4.2 Analisar e emitir Parecer para a Diretoria Colegiada sobre a implantação, ajustes, atualizações e outras proposições relacionadas às Política e Normas de Segurança da Informação e Privacidade, encaminhados pelo Responsável pela Segurança da Informação e Privacidade;

5.5 Responsável pela Segurança da Informação e Privacidade

5.5.1 Monitorar e acompanhar o cumprimento dessa Política, encaminhando aos Gestores das unidades as ocorrências de descumprimento das normas de segurança por seus empregados e colaboradores para as providências cabíveis, cientificando a GECOR;

5.5.2 Tomar as providências de emergência conforme estabelecido no Plano de Ação de Resposta a Incidentes, imediatamente após detecção ou conhecimento de incidentes de segurança no âmbito do ambiente da empresa, notificando o ocorrido à Diretoria, GECOR e à Auditoria Interna tempestivamente;

5.5.3 Identificar e propor medidas e contramedidas necessárias para correção de problemas causados por quebra ou fragilidade da Política de Segurança da Informação, Privacidade;

5.5.4 Propor programas de treinamentos, tendo como objetivo a capacitação dos Administradores, membros dos Órgãos Estatutários, Empregados e Colaboradores dos ativos de tecnologia da informação, visando o cumprimento da Política de Segurança da Informação e Privacidade;

5.5.5 Divulgar de forma sistemática informações que contribuam para a conscientização dos Administradores, membros dos Órgãos Estatutários, Empregados e Colaboradores para a importância da existência e do cumprimento da Política de Segurança da Informação e Privacidade;

5.5.6 Implementar ações referentes à Gestão de Segurança da Informação e Privacidade decorrentes das deliberações da Diretoria Colegiada;

5.5.7 Zelar pela aplicação efetiva das melhores práticas em Segurança da Informação e Privacidade;

5.6 Gerência da Tecnologia da Informação – GETI

5.6.1 Gerenciar os ativos de tecnologia da informação, visando cumprir a Política de Segurança da Informação e Privacidade;

5.6.2 Participar em conjunto com a responsável pela segurança e privacidade sobre o planejamento das atividades relacionadas à Gestão de Segurança da Informação, Privacidade e Cibersegurança;

5.6.3 Configurar os equipamentos, ferramentas e sistemas concedidos aos Administradores, membros dos Órgãos Estatutários, Empregados e Colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSIP;

5.6.4 Garantir segurança para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação;

5.6.5 Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes;

5.6.6 Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a AFEAM;

5.6.7 Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela;

5.6.8 Proteger continuamente todos os ativos de informação da organização contra código malicioso e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

5.7 GECOR

5.7.1 Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações;

5.7.2 Garantir que medidas corretivas sejam tomadas quando desconformidades forem identificadas;

5.7.3 Avaliar o nível de segurança alcançado, emitindo, semestralmente Relatório de Posição à Diretoria Colegiada.

5.7.4 Monitorar e avaliar a conformidade da Política

5.8 Auditoria Interna – AUDIN

5.8.1 Realizar auditoria de verificação de conformidade relacionada à essa Política ao menos uma vez ao ano, emitindo o respectivo Relatório de Auditoria e submetendo-o a apreciação da Diretoria Colegiada;

5.8.2 Avaliar e emitir Parecer para a Diretoria Colegiada sobre os incidentes de segurança reportados pela GECOR, e pelas demais áreas;

5.8.3 Propor a criação de novos controles e/ou ajustes de controles já existentes, visando eliminar ou minimizar a ocorrência de incidentes de segurança da informação, privacidade e cibersegurança.

5.9 Gerência Jurídica – GEJURI

5.9.1 Auxiliar o CSIP e demais unidades da AFEAM, quanto aos aspectos legais referentes à Gestão de Segurança da Informação e Privacidade;

5.9.2 Tomar as providências jurídicas cabíveis em casos de incidentes de Segurança da Informação e Privacidade, quando solicitado pelo CSIP;

5.9.3 Revisar os contratos (modelos e minutas) garantindo a existência de cláusulas referentes à confidencialidade e segurança das informações conforme legislação e regulamentações vigentes, como a Lei Geral de Proteção de Dados (LGPD);

5.9.4 Fornecer ao Comitê de Segurança da Informação e Privacidade – CSIP orientações a respeito da conformidade legal nos seguintes temas:

- Direitos de Propriedade Intelectual;
- Proteção de Registros Organizacionais;
- Proteção de Dados e Privacidade de Informações Pessoais;
- Prevenção de mau uso de Recursos de Processamento de Informação;
- Segurança da Informação e Privacidade;
- Guarda de registros de conexão e dados cadastrais;
- Combate a corrupção;
- Outros relacionados ao tema.

5.10 Gerência de Gestão de Pessoas e Contratos – GEPEC

5.10.1 Auxiliar o Responsável pela Segurança da Informação na elaboração e execução de Programa de Treinamento que trata da Segurança da Informação e Privacidade;

5.10.2 Providenciar que todos os Administradores, membros dos Órgãos Estatutários, Empregados e Colaboradores recebam instruções sobre sua responsabilidade pela Segurança da Informação e Privacidade, com os aspectos culturais, missão, visão, valores, normas, regulamentações, políticas, direitos e deveres que são esperados dele na AFEAM, assinando o Termo de Compromisso;

5.10.3 No caso de terceiros, como órgãos fiscalizadores, que necessitem ter acesso a informações e dados pessoais dos Administradores, membros dos Órgãos Estatutários, Empregados, Colaboradores e Clientes, os mesmos devem ser informados quanto ao sigilo das informações, seja no corpo do e-mail ou correspondências (Ofício), dando ciência.

5.10.4 Solicitar a devolução dos ativos de TI da AFEAM ou qualquer documento e a retirada de acesso de todos os Administradores, membros dos Órgãos Estatutários, Empregados e Colaboradores no encerramento de suas atividades, contratos ou acordos;

5.11 Gestores das Unidades

5.11.1 Colaborar com o Responsável pela Segurança da Informação e Privacidade na formulação de propostas de implantação, ajustes, atualizações e/ou demais proposições na Política e Normas relacionados à Política de Segurança da Informação e Privacidade;

5.11.2 Cumprir e fazer cumprir a Política de Segurança da Informação e Privacidade por seus empregados e colaboradores;

5.11.3 Notificar ao Responsável pela Segurança da Informação e Privacidade sobre incidentes de segurança ocorridos ou em eminência de ocorrer em sua unidade de atuação ou em outras unidades, tempestivamente;

5.11.4 Solicitar a criação de perfis de acesso ao ambiente de tecnologia da informação e às dependências da AFEAM às unidades responsáveis;

5.11.5 Respeitar e cumprir esta Política e seus documentos complementares;

5.11.6 Sugerir medidas que possam elevar o nível de segurança da informação e privacidade das instalações em sua unidade de atuação.

5.11.7 Responder pela integridade dos ativos de informação, de propriedade da AFEAM ou não, colocados à disposição para exercer suas atividades;

5.11.8 Responder pelo uso exclusivo e intransferível de suas senhas de acesso;

5.11.9 Relatar prontamente à Encarregado de Dados qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, violação de dados pessoais ocorridos ou em iminência de ocorrer em sua unidade de atuação ou em outras unidades;

5.11.10 Assegurar que as informações e dados de propriedade da AFEAM não sejam disponibilizados a terceiros, ou pelo menos, sem a devida autorização por escrito do responsável hierárquico;

6. Disposições Finais

6.1 Os incidentes de segurança da informação e privacidade identificados devem ser avaliados pelo CSIP, sendo constatado deve-se encaminhar um relatório para Diretoria Colegiada, que após análise, poderá instaurar e apurar as responsabilidades dos envolvidos, por meio de Procedimento Administrativo Disciplinar, visando aplicação de sanções administrativas cabíveis previstas no Código de Ética, Conduta e Integridade da AFEAM, em outros manuais internos além da legislação vigente;

6.2 A tentativa de burlar às diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação;

6.3 A não observância dos princípios e diretrizes constantes nesta política e seus documentos complementares, pode impactar seriamente a AFEAM, possibilitar a violação de leis e regulamentos, e afetar negativamente a reputação e a estabilidade financeira da AFEAM. Desvios e exceções devem ser tratados pelo Comitê de Segurança da Informação e Privacidade – CSIP.

7. Políticas e Normas Complementares

a) Política de Privacidade Externa – Público em Geral;

b) Política de Privacidade Interna;

c) Política de Atendimento a Titulares;

d) Política de Proteção de Dados;

e) Política de Retenção e Descarte de Dados Pessoais;

f) Política de Adequação de Contratos com Terceiros;

g) Política de Classificação da Informação;

h) Política de Gestão de Mudanças;

i) Política de Contratação de Serviços em Nuvem;

j) Política de Uso de Dispositivos Móveis Corporativos da AFEAM;

k) Norma de Backup e Restauração;

l) Norma de Uso de Ativos de Tecnologia da Informação;

m) Norma de Acesso Remoto;

n) Norma de Controle de Acesso e Senhas;

o) Norma de Uso de Dispositivos Móveis;

p) Norma de Gestão de Vulnerabilidades;

q) Norma de Desenvolvimento Seguro;

r) Norma de Controle Criptográfico;

s) Norma de Gestão de Monitoramento;

t) Norma de Segmentação de Redes;

u) Norma de Monitoramento e Tratamento de Incidentes;

v) Norma de Descarte e Destruição de Informações;

w) Norma de Acesso ao Meio Físico;

x) Norma de Segurança em Recursos Humanos;

y) Norma de Uso de Mensageiros e Comunicadores Instantâneos;

z) Norma de Uso de Redes Sociais.

8. Atualização

A AFEAM reserva-se no direito de atualizar esta política sempre que ocorrerem alterações na legislação vigente ou procedimentos que afetem seu conteúdo.

9. Documentos de Referência

- Lei nº 13.709/2018: Lei Geral de Proteção de Dados Pessoais - LGPD;
- ABNT NBR ISO/IEC 27001:2013: Tecnologia da Informação — Técnicas de Segurança — Sistemas de Gestão da Segurança da Informação — Requisitos;
- ABNT NBR ISO/IEC 27002:2013: Tecnologia da Informação — Técnicas de Segurança — Código de Prática para Controles de Segurança da Informação;
- ABNT NBR ISO/IEC 27032:2015: Tecnologia da Informação — Técnicas de Segurança — Diretrizes para Segurança Cibernética;
- ABNT NBR ISO/IEC 27701:2019: Tecnologia da Informação — Técnicas de Segurança — Extensão à ABNT NBR ISO/IEC 27002 para Gestão da Privacidade da Informação – Requisitos e Diretrizes.

AFEAM

Agência de Fomento do
Estado do Amazonas S.A.