PLANO GERAL DE AÇÃO **LEI GERAL DE PROTEÇÃO DE DADOS**

AGOSTO 2022

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

DE DADOS 13.709/2018

ABAPA - ASSOCIAÇÃO BAIANA DOS PRODUTORES DE ALGODÃO

DESENVOLVIDO POR:

Núcleo de Proteção de Dados do Oeste da Bahia.
Pacheco e Queiroz

Sumário

1. CONTEXTUALIZAÇÃO

A **ABAPA,** empresa consciente da importância de resguardar e proteger os dados pessoais que estão sob sua guarda, apresenta a presente **Política de Segurança da Informação**.

Amparada nos preceitos da norma técnica “NBR ISSO/IEC 27002 – Código de prática para a gestão da segurança da informação”, esta Política traz diretrizes gerais de conduta, bem como obrigações a serem seguidas pela **ABAPA**, a fim de mitigar eventuais riscos e danos relacionados a ameaças externa ou internas, deliberadas ou acidentais, que possam impactar na confidencialidade, integridade e disponibilidade das informações de qualquer natureza, objetivando garantir sua preservação.

2. SEGURANÇA DA INFORMAÇÃO

Segurança da Informação é a proteção da Informação contra vários tipos de ameaças, para garantir a continuidade do negócio, minimizando os riscos e maximizando o retorno sobre os investimentos e as oportunidades para a **ABAPA** e seus clientes. Ela é obtida a partir da implementação de um conjunto de controles, incluindo tecnologia, políticas, processos, procedimentos e a própria estrutura organizacional da empresa.

Os controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente, sempre que necessários, e melhorados continuamente para garantir que os objetivos e a segurança da **ABAPA** sejam atendidos.

Internamente, considera-se como informação toda a base de conhecimento, conteúdo, dado, conceito, envio ou recebimento de mensagem, processo ou fato existente, em meio físico ou eletrônico, que compõe documentos e informações de propriedade, interesse ou posse da **ABAPA** e inclui, mas não se limita a, qualquer dado, material, procedimento, processo, especificações, inovações e aperfeiçoamento técnicos e comerciais que agreguem valor para o negócio da empresa, assim como todas as informações confidenciais dos nossos clientes sob nossa custódia.

3. CLASSIFICAÇÃO DA INFORMAÇÃO.

A informação é tida como um ativo e possui valor diferente dependendo do seu conteúdo. Os controles de proteção desses ativos podem aumentar de acordo com seu valor. A classificação das informações também pode definir quais controles de proteção precisam ser implementados. Assim a classificação da Informação é feita numa escala de proteção a ser aplicada, sendo elas:

a) **Públicas:** são todas as informações que já sejam de conhecimento público e estejam disponibilizadas para clientes, colaboradores e público em geral, por meio da Internet, ou veiculadas em documentos publicados em jornais, revistas, folders, redes sociais, panfletos, avisos ou palestras autorizadas.

b) **Internas:** são informações que estão disponíveis aos colaboradores por meio das ferramentas aprovadas, com armazenamento interno, em servidores da **ABAPA** ou terceiros autorizados (na nuvem, por exemplo). Qualquer informação classificada como "INTERNA" não poderá ser encaminhada, divulgada ou publicada em quaisquer meios para terceiros não autorizados, devendo a sua disponibilização ser restrita ao ambiente de trabalho da empresa e uso limitado aos colaboradores ou terceiros (mediante assinatura de termo de "não divulgação" - NDA), que realmente necessitem ter acesso a tais informações.

c) **Restritas:** são os documentos que somente poderão ser acessados pela área, departamento, setor ou função dentro da **ABAPA** que classificou a informação. Normalmente são informações de uma determinada área que não deve ser acessada por outros setores da empresa.

d) **Confidencial:** são as informações que deverão ser mantidas em arquivos físicos ou eletrônicos com níveis de segurança compatíveis com a relevância da informação, tais como cofres, armários com chaves, diretórios criptografados ou envio dos arquivos somente após a inclusão de mecanismos de segurança (senha ou criptografia). A transmissão de arquivos confidenciais só deverá ser feita utilizando meios de transmissão seguras, para as partes previamente autorizadas, com contrato de sigilo claro e dentro da validade.

e) **Secretas:** as Informações classificadas como SECRETAS possuem o mais alto nível de sensibilidade e criticidade para o negócio. Chaves de criptografia (certificados SSL, A1, A3 ou chaves SSH) e credenciais de acesso em geral são exemplos de Informações SECRETAS. Outras Informações estratégicas com alto nível de confidencialidade também pode ser classificadas como SECRETAS a critério do proprietário da Informação.

   Informações em que seu possível vazamento implica em impacto financeiro direto ao negócio ou ponha em risco a continuidade dos negócios é um indício para que ela receba a classificação máxima de proteção: SECRETA.

   As Informações SECRETAS normalmente possuem os seguintes controles e proteções:

   - *São armazenadas em volumes criptográficos acrescidos de criptografia de arquivo: criptografia multinível com chaves e algoritmos distintos.*

- As Informações SECRETAS não podem ser copiadas, fotografadas, filmadas (incluindo sistemas de CFTV) ou testemunhadas, pessoalmente ou por meio de telepresença de qualquer forma, o sistemas de CFTV são considerados nessa política informações SECRETAS e seus acessos são de uso exclusivo e restrito do time de segurança patrimonial, cabendo eles a gestão de senha dos mesmo.
- Gestor Geral, e o Financeiro.
- Algumas Informações SECRETAS podem simplesmente não ser armazenadas (*Brian store Only*), processadas ou transmitidas no ambiente computacional do Enalta sempre que isso for possível.
- O armazenamento das Informações SECRETAS só pode ocorrer em regime de exceção em sistemas offline ou sistemas online aprovados nesta Política:

    a. **Senhas e Credenciais** corporativas de acesso: só poderão ser armazenadas na sua memória ou por meio de software de gestão de senhas (PREFERENCIALMENTE. Ex.: Lastras).
    b. Quaisquer senhas armazenadas nos sistemas internos aprovados, para colaboradores e clientes só deverão ser armazenadas utilizando conversão em HASH (SHA256 ou superior) adicionada de técnicas de SALT, técnicas conhecidas como boas práticas de segurança mínima para armazenamento de senhas. Deste modo, TODAS AS SENHAS dentro dos sistemas de Informações do Grupo ABAPA, para acesso interno ou externo (pelos clientes por exemplo), somente são conhecidas pelo seu proprietário. Nem o Diretor Presidente do Grupo ABAPA possui acesso à senha de qualquer usuário dos sistemas internos a não ser o proprietário da conta de acesso (cliente ou colaborador).
    c. Tamanho de senha mínimo recomendável: mínimo de 9 caracteres e obrigação do uso de 4 opções (maiúsculo, minúsculo, caractere especial e numeral). Também serão aplicadas restrições a palavras comuns como: Enalta, Petróleo, Gás e etc.

HASH: função criptográfica de via única em que uma sequência de dados gera uma saída única de tamanho fixo que não pode ser revertida. Ou seja, conhecendo o HASH não é possível conhecer a Informação que o gerou.

SALT: trata-se de uma técnica para aumentar a segurança do HASH e evitar ataques do tipo dicionário, onde de posse de um banco de dados de palavras e seus respectivos HASH, se possa chegar à sequência, neste caso a senha em formato aberto.

				Secreta
			Confidencial	
		Restrita		
	Interna			
Pública				

A classificação dos documentos deverá ocorrer em campo visível, preferencialmente na primeira página e próximo ao cabeçalho do Documento.

Quando um Documento contiver mais de um tipo de Informação com classificação original distintas, por exemplo, dois documentos unidos em um único arquivo, a classificação mais restritiva passa a valer para todo o documento.

Qualquer Informação que não tenha sua classificação especificada de forma clara no documento será automaticamente considerada como Informação “RESTRITA”.

4. DEFINIÇÕES

AMEAÇA: evento que tem potencial em si próprio para comprometer os objetivos da **ABAPA,** seja trazendo danos direitos aos ativos ou prejuízo indiretos decorrentes de situações inesperadas.

ATIVOS DE INFORMAÇÃO: são os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, os locais onde se encontram esses meios, as pessoas que têm acesso a informação, assim como as próprias informações coletavas, produzidas, processadas, armazenadas, custodiadas, descartadas e transmitidas pela **ABAPA.**

AUTENTICIDADE: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

CLASSIFICAÇÃO DA INFORMAÇÃO: identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identifica-las, além de determinar os controles de proteção necessários a cada uma delas.

CONFIDENCIALIDADE: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizados e credenciados.

CONFORMIDADE: processo que visa verificar o cumprimento das normas estabelecidas.

CONTROLE DE ACESSO: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.

CRIPTOGRAFIA: método de codificação da informação que visa evitar que ele seja compreendida ou alterada por pessoas não autorizadas.

CUSTODIANTE DO ATIVO DE INFORMAÇÃO: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia.

DADOS PESSOAIS: toda e qualquer informação relacionada a um indivíduo (pessoa natural) que possa ser identificada ou identificável, direta ou indiretamente, ou quando combinadas, produzem resultado de identificação do sujeito.

DISPONIBILIDADE: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade no momento requerido.

GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO – GRSI: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos da informação.

GDPR: *General Data Protection Regulation*: conjunto de regras sobre tratamento de dados aprovado em 2016 válido para a União Europeia (EU). Regulamenta também a exportação de dados pessoais para fora da EU.

INFORMAÇÃO: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que reside ou da forma pela qual seja veiculado.

INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO: instalações prediais (energia, água, climatização, acesso físico), computadores e equipamentos, software, redes e telecomunicações, sistemas de armazenamento e recuperação de dados (arquivos e armazenamento), aplicações computacionais, cabeamento e rede telefônica.

INTEGRIDADE: propriedade de que a informação não foi modificada, suprimida ou destruída de maneira não autorizada ou acidental.

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD): Lei nº 13.709/2018, que dispõe sobre o tratamento de dados pessoais, em meios físicos ou digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado.

PARCEIROS COMERCIAIS: toda pessoa física ou jurídica que possui relações comerciais, independentemente de como essa relação se estabeleceu, seja por contrato de parceria, prestação de serviços ou outros.

SOFTWARE MALICIOSO: trata-se de qualquer software que realiza ações nocivas aos sistemas, como vírus, cavalo de troia, verme (worm) e afins.

TERCEIRO: é toda pessoa física ou jurídica contratada pela **ABAPA** para desenvolver ou auxiliar no desenvolvimento de suas atividades.

TRATAMENTO DA INFORMAÇÃO: conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação.

VÍRUS MALICIOSO: entende-se por vírus qualquer programa que tem a capacidade de se reproduzir automaticamente, sem o conhecimento ou autorização do usuário

VULNERABILIDADE: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

5. ESCOPO

A Política de Segurança da Informação tem como escopo estabelecer diretrizes para resguardar e proteger as informações – sejam elas pessoais ou não – que estão sob a guarda da **ABAPA**, além de definir a governança de segurança da informação da empresa, observando o que determina todas as leis e regulamentações aplicáveis e em vigor relacionadas a proteção de dados, especialmente a LGPD e a GDPR.

6. ABRANGÊNCIA

A Política de Segurança da Informação alcança todos os processos que de alguma forma tratam dados pessoais analógicos e digitais dos titulares que se relacionam com a **ABAPA**, aplicando, assim, a todas as pessoas que trabalham na empresa, sejam diretores, contadores, assessores, profissionais de qualquer natureza, estagiários e aprendizes, bem como para

qualquer pessoa física ou jurídica, de Direito Público ou Privado, com quem se relaciona: prestadores de serviços, parceiros, clientes, entre outros.

Todas os destinatários deverão observar as presentas regras e recomendações em quaisquer operações que possam impactar na segurança das informações da **ABAPA**, sob pena das medidas previstas nessa Política, sem prejuízo das previstas em lei.

7. APLICABILIDADE

Esta Política de Segurança da Informação estabelece diretrizes e regras para garantir que seus destinatários entendam e cumpram as legislações que versam sobre a proteção de dados pessoais, bem como os padrões e medidas técnicas visando a segurança da informação na **ABAPA.**

8. OBJETIVOS

São objetivos da presente Política de Segurança da Informação da **ABAPA**:

a) estabelecer as diretrizes que assegurem e reforcem o compromisso da **ABAPA** com as práticas e medidas preventivas garantidoras de segurança da informação;
b) definir o referencial para a normatização das questões de segurança da informação na **ABAPA**;
c) criar condições para que a **ABAPA** eleve continuamente a sua maturidade em segurança da informação por meio da adoção de diretrizes, normas e procedimentos destinados a proteger os ativos de informação da empresa, visando a promoção da integridade, confidencialidade, autenticidade e disponibilidade dos ativos de informação;
d) prover a **ABAPA** de mecanismos de atendimento e conformidade às leis de segurança da informação, nacionais e internacionais;
e) descrever as regras comportamentais e diretrizes a serem seguidas na condução das atividade desenvolvidas pela **ABAPA** que garantem a prevenção de incidentes de segurança da informação e a proteção de dados pessoais.

9. PRINCÍPIOS

O compromisso da **ABAPA** com o tratamento adequado das informações se baseia nos seguintes princípios:

a) **Autenticidade**: todos os esforços serão feitos para que as informações sejam confiáveis e corretas, ou seja, as informações não serão alteradas de forma não autorizadas ou indevidas;
b) **Confidencialidade**: o acesso à informação é permitido somente as pessoas autorizadas e quando ele for de fato necessário;
c) **Disponibilidade**: somente as pessoas autorizadas têm acesso à informação sempre que necessário;
d) **Integridade**: todos os esforços serão feitos para que as informações sejam exatas e completas, bem como seu processamento.

10.DIRETRIZES GERAIS

10.1 Acesso à informação

A informação sob custódia **ABAPA**, mesmo que pertencente a clientes ou fornecedores, deve ser protegida contra o acesso de pessoas não autorizadas.

A geração, utilização, armazenamento, manutenção, distribuição e destruição da informação devem ser feitas de acordo com as necessidades da empresa, sendo que estes processos devem estar devidamente documentados.

A **ABAPA** reserva-se o direito de consultar e analisar informações armazenadas em suas dependências e em seus equipamentos, bem como em malotes, envelopes, arquivos físicos e eletrônicos, geradas ou recebidas com utilização de seus recursos humanos e materiais.

Devem ser usados somente recursos autorizados para garantir o compartilhamento seguro da informação quando for necessário.

A informação deve ser armazenada, pelo tempo determinado pela **ABAPA** ou pela legislação vigente, o que for maior, e recuperável quando necessário. O local de armazenamento das informações deve ser apropriado e protegido contra sinistros e acessos de pessoas não autorizadas.

10.2 Acesso à informação

O uso de redes externas de comunicação (Internet, redes privadas, etc.) da **ABAPA** é controlado através de Servidores de Firewalls, Servidores de Acesso à Internet, ferramentas de

Antivírus e políticas de sistemas operacionais / que garantam que somente os recursos necessários estejam disponíveis para o trabalho, sem riscos para o ambiente operacional.

O acesso externo aos sistemas da organização, quando realizado pelo pessoal da Área de Suporte Técnico ou por prestadores de serviço, deve ser controlado e restrito aos serviços necessários, mantendo trilhas de utilização e restringindo-se ao mínimo necessário. A solução encontrada para cada caso deve ser formalizada e documentada através do e-mail para o governança local, ti@abapa.com.br, o mesmo acesso deverá ser concedido apenas pelas plataformas homologadas.

A remessa de dados da **ABAPA**, seja para atender requisitos de negócio, como para viabilizar a resolução de problemas encontrados, deve ser avaliada em função dos riscos e pela adoção de procedimentos que garantam o controle e a integridade dos dados, além da legitimidade do receptor das informações. O que for acordado deve ser formalizado e aprovado pelos gestores responsáveis pela informação.

10.3 Sistemas aplicativos

Sistemas aplicativos desenvolvidos dentro da **ABAPA** devem ser documentados e controlados quanto às alterações ou correções feitas, com trilhas do que foi feito e guarda segura da biblioteca de fontes. Toda informação necessária para eventual reconstrução dos aplicativos deve constar de sua documentação.

Sistemas aplicativos desenvolvidos fora da **ABAPA**, de propriedade de terceiros (com licença de uso para a organização), devem ter a biblioteca de fontes e de recursos adicionais (bibliotecas adquiridas, componentes, etc.) sob custódia de uma entidade idônea, de comum acordo entre a organização e a empresa fornecedora do software.

Tais fontes devem sempre ser atualizadas e verificadas quanto à sua validade e sincronização com a versão em uso no ambiente de produção.

O mau uso dos sistemas, feito de forma acidental ou deliberada, deve ser combatido. Ademais, para minimizar o risco de falhas nos sistemas deve-se fazer um planejamento e preparações prévias para garantir a disponibilidade e capacidade adequada dos recursos.

10.4 Diretrizes Específicas

Para cada um dos controles complementares propostos pela NBR ISO/IEC 27002 – Código de prática para a gestão da segurança da informação, a Diretoria da **ABAPA** deve elaborar estratégias, diretrizes e normas de procedimento complementares, assim como manuais, procedimentos de conduta e avaliações periódicas de conformidade.

A presente Política de Segurança da Informação preconiza a implantação priorizada das seguintes normas de procedimento com as seguintes diretrizes:

10.5 Gestão de ativos de informação

Entende-se por ativo tudo aquilo que a **ABAPA** considerar como relevante para o negócio, desde ativos tecnológicos (p.ex. software e hardware).

Os ativos, de acordo com sua criticidade, devem ser identificados, inventariados, mantidos atualizados, através de planilhas ou relatórios de softwares, possuírem um proprietário e serem protegidos conta acessos indevidos. A proteção pode ser física (p.ex. salas com acesso controlado). Ademais, os ativos de informação devem ser monitorados e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos.

Os ativos da **ABAPA** devem ser tratados de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, promovendo o uso adequado e prevenindo exposição indevida das informações.

Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

O acesso dos usuários aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado ao aceito a termo de sigilo e responsabilidade.

10.6 Segurança em recursos humanos

Todas pessoas com acesso aos sistemas e informações da **ABAPA** devem ter ciência das ameaças e preocupações relativas à segurança da informação e de suas responsabilidades e obrigações no âmbito desta Política de Segurança da Informação. Além disso, devem difundir e exigir o cumprimento desta Política, das normas de segurança e da legislação vigente acerca do tema.

Todos as pessoas com acesso aos sistemas e informações da **ABAPA** deverão ter uma única identificação (*login*) e senha pessoal e intrasferível, devendo as exceções serem devidamente documentadas.

Todos os colaboradores devem assinar o Termo de Responsabilidade, a qual se trata de um compromisso de responsabilidade direta desse para com as informações, equipamentos e outras propriedades da **ABAPA** a ele confiadas, devendo ser lida e assinada quando de sua admissão. Ademais, todos os colaboradores, prestadores de serviço e terceiros devem assinar

um Termo de Confidencialidade, que valerá durante todo o período de vínculo com a empresa e, adicionalmente, terá duração de 05 (cinco) anos, contados após o término deste vínculo.

A presente Política de Segurança da Informação deve constar em cláusula contratual nos contratos de terceiros.

O termo de aceite e a política de segurança da informação devem ser incluídos como anexos do contrato.

10.7 Gestão de riscos e incidentes

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

Os prestadores de serviços e parceiros da **ABAPA** devem informar os incidentes relevantes, relacionados às informações armazenadas ou processadas por eles em cumprimento às determinações legais e regulamentares.

Produtos, processos e tecnologias devem ter a adequada gestão dos riscos de Segurança da Informação, para redução dos riscos à níveis aceitáveis, independentemente de estarem dentro da infraestrutura da **ABAPA**, parceiros ou prestadores de serviços.

As tecnologias em uso pela **ABAPA** devem estar em versões suportadas pelos seus fabricantes e devidamente atualizadas. Eventuais exceções devem ser aprovadas na alçada competente ou possuir controles compensatórios.

10.8 Gestão de acessos

Todo acesso às informações e aos ambientes lógicos e físicos da **ABAPA** deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas pelo respectivo proprietário da informação.

A política de controle de acesso deve ser documentada e formalizada por meio de normas e procedimentos que contemplem, pelos menos, os seguintes itens:

a) Procedimento formal de concessão e cancelamento de autorização de acesso do usuário aos sistemas de informação;
b) Comprovação da autorização do proprietário da informação;
c) Utilização de identificadores de usuário (ID de usuário) individualizados, de forma a assegurar a responsabilidade de cada usuário por suas ações;

d) Verificação se o nível de acesso concedido é apropriado ao propósito do negócio e se é consistente com a Política de Segurança da Informação, as normas e procedimentos;
e) Remoção imediata de autorização dadas a usuários afastados ou desligados da empresa, ou que tenham mudado de função deverá ser comunicado imediatamente ao time de Governança de T.I para fazer os ajustes de retirada e liberação;
f) Processo de revisão periódica das autorizações concedidas;
g) Política de atribuição, manutenção e uso de senhas.

Além desses itens, as normas devem prever a respeito da identificação do usuário, que, qualquer que seja o meio e a forma, deve ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento.

10.9 Gestão de continuidade de negócios

O processo de gestão de continuidade de negócios da **ABAPA** é estabelecido por um conjunto de políticas, normas e práticas operacionais que seguem os princípios da NBR ISO/IEC 27001/2 – Código de prática para a gestão da segurança da informação, cujo objetivo é garantir que os processos críticos tenham continuidade, atendendo aos requisitos mínimos operacionais e evitando impactos nos negócios e nos seus clientes.

10.10 Gestão de conformidade

O processo de conformidade das práticas de segurança da informação da **ABAPA** se dá com a presente Política de Segurança da Informação, bem como com a legislação específica da informação.

A verificação de conformidade deve também ser realizada nos contratos e outros instrumentos do mesmo gênero celebrados com a empresa.

Nenhum setor da **ABAPA** pode permanecer sem verificação de conformidade de suas práticas de segurança da informação por período superior a 2 (dois) anos.

Os resultados de cada ação de verificação de conformidade são documentados em relatório de avaliação de conformidade, o qual será encaminhado pelo Diretor da empresa.

11. PAPÉIS E RESPONSABILIDADES

1.1 Diretoria

a) Cumprir esta Política de Segurança da Informação e demais documentos complementares por todos os colaboradores de **ABAPA;**
b) Analisar e aprovar a Política de Segurança da Informação e demais documentos complementares;
c) Orientar para que as atividades desempenhas pelo Responsável pela Segurança da Informação estejam adequadas ao negócio da **ABAPA;**
d) Instaurar, quando couber, procedimento disciplinar para apuração de responsabilidades dos envolvidos em violações de segurança da informação.

1.2 Responsável pela Governança de Segurança da Informação

a) Cumprir e fazer cumprir esta Política de Segurança da Informação e demais documentos complementares por todos os colaboradores da **ABAPA;**
b) Definir, analisar e priorizar ações necessárias, balanceando custo e benefício;
c) Promover a capacitação dos colaboradores em segurança de informação;
d) Autorizar o uso de recursos de Tecnologia da Informação particulares para execução das atividades profissionais;
e) Analisar os incidentes de segurança da informação reportados e submeter relatório para deliberação da Diretoria. (Plano de Resposta Incidente)

1.3 Responsável pela Tecnologia da Informação

a) Realizar a gestão e manutenção dos Recursos de Tecnologia da Informação de propriedade da **ABAPA** ou que estão sob sua responsabilidade;
b) Identificar e avaliar os riscos relacionados à segurança da informação nos Recursos de Tecnologia da Informação e propor melhorias, quando couber;
c) Garantir que todos os Recursos de Tecnologia da Informação da **ABAPA** atendam as recomendações de seus fabricantes ou desenvolvedores;
d) Disponibilizar e realizar a gestão das identidades digitais de acesso ao ambiente lógico da **ABAPA;**
e) Mapear e inventariar os Recursos de Tecnologia da Informação da **ABAPA**;
f) Realizar o registro e o monitoramento dos acessos aos ambientes lógicos da **ABAPA**;
g) Realizar a inspeção dos Recursos de Tecnologia da Informação, sempre que considerar necessário e justificado;
h) Avaliar se os requisitos de segurança da informação estão presentes antes da aquisição ou desenvolvimento de softwares;
i) Realizar o processo de manutenção nos Recursos de Tecnologia da Informação da **ABAPA**, sempre que solicitado;

j) Garantir que o andamento e o resultado de uma mudança, principalmente nos sistemas e infraestrutura tecnológica da **ABAPA**, preservem os controles relacionados a disponibilidade, integridade, sigilo e autenticidade das informações;
k) Elaborar e manter mecanismos adequados para garantir a rápida recuperação em situações de contingência de seus sistemas e processos que envolvam os Recursos de Tecnologia da Informação da **ABAPA**;
l) Elaborar e manter procedimentos de salvaguarda das informações dos Recursos de Tecnologia da Informação críticos da **ABAPA**;
m) Assegurar que os procedimentos de Gestão da Continuidade de Negócios sejam executados em conformidade com os requisitos de segurança da informação.

1.4 Responsável pelas questões jurídicas

a) Ser envolvido previamente em todos os processos de contratação, validando as minutas que devem estar alinhadas aos controles de segurança da informação aplicáveis.

1.5 Responsável pelos recursos humanos

a) Apoiar o responsável em segurança da informação nas campanhas de capacitação e divulgação da segurança da informação;
b) Estipular controles de segurança especificamente relacionados aos processos de contratação, encerramento e modificação das atividades;
c) Informar sobre a Política de Segurança da Informação na ocasião da admissão do novo colaborador e colher assinatura do Termo de Compromisso;
d) Em caso de desligamento, informar de forma antecipada a Remoção imediata de autorização dadas da empresa dos acessos concedidos, deverá ser comunicado imediatamente ao time de Governança de T.I para fazer os ajustes de retirada e liberação.

1.6 Colaboradores

a) Cumprir e manter-se atualizado com esta Política de Segurança da Informação e demais documentos complementares;
b) Conhecer “Termo de Responsabilidade” e o “Termo de Confidencialidade” e assinar o documento de Cláusula de Segurança de Informação para o Contrato de Trabalho;
c) Utilizar de forma profissional, ética e legal as informações e os Recursos de Tecnologia da Informação da **ABAPA**, respeitando os direitos e as permissões de uso concedidas;
d) Preservar a integridade, a disponibilidade, a confidencialidade, autenticidade e a legalidade das informações acessadas ou manipuladas, não as utilizando, enviando, transmitindo ou compartilhando indevidamente, em qualquer local ou mídia, inclusive na Internet;
e) Não revelar qualquer informação de propriedade ou sob a responsabilidade da **ABAPA** sem a prévia e formal autorização;

f) Utilizar todos os ativos, tangíveis e intangíveis da **ABAPA**, quando autorizados, somente para fins profissionais;
g) Não utilizar as marcas, a identidade visual ou qualquer outro sinal distintivo, atual e futuro, da **ABAPA** em qualquer forma ou mídia, inclusive na Internet e nas mídias sociais, sem a prévia e formal autorização para tanto;
h) Zelar pela segurança da sua identidade digital, não compartilhando, divulgando ou transferindo a terceiros;
i) Responder por toda e qualquer atividade realizada nos Recursos de Tecnologia da Informação da **ABAPA** realizada mediante o uso de suas credenciais de acesso;
j) Cumprir a legislação nacional vigente e demais instrumentos regulamentares relacionados às atividades profissionais;
k) Reportar formalmente ao Responsável da Segurança da Informação quaisquer eventos relativos à violação ou possibilidade de violação de segurança de informação ou atividades suspeitas.

1.7 Terceiros e parceiros comerciais

a) Tomar conhecimento e seguir as diretrizes estabelecidas pela **ABAPA** em relação a segurança da informação;
b) Reportar formalmente ao Responsável da Segurança da Informação quaisquer eventos relativos à violação ou possibilidade de violação de segurança de informação ou atividades suspeitas.

12. RECOMENDAÇÕES

12.1 Recomendações para o uso aceitável dos recursos de Tecnologia da Informação

O uso correto e responsável dos recursos de Tecnologia da Informação deve ser aplicado a todos colaboradores da **ABAPA**.

Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas no âmbito da infraestrutura de TI, ficando os transgressores sujeitos as penalidades descritas na legislação vigente.

Os documentos produzidos por intermédio dos sistemas de TI são de propriedade da **ABAPA**.

Os sistemas de TI deverão ser utilizados sem violação dos direitos de propriedade intelectual de qualquer pessoa ou empresa, como marcas e patentes, nome comercial, segredo

empresarial, domínio na Internet, desenho industrial ou qualquer outro material, que não tenha autorização expressa do autor ou proprietário dos direitos, relativos à obra artística, científica ou literária.

As informações pertencentes à empresa devem ser utilizadas apenas para os propósitos definidos na sua missão institucional.

12.2 Recomendações para o uso seguro dos recursos de Tecnologia da Informação

Recomenda-se aos colaboradores da **ABAPA** a adoção das seguintes práticas:

a) Fazer regularmente cópias de segurança de seus dados;
b) Manter registro das cópias de segurança;
c) Guardar as cópias de segurança em local seguro e distinto daquele onde se encontra a informação original;
d) Utilizar senhas que contenham, pelo menos, oito caracteres, compostos de letras, números e símbolos, evitando o uso de nomes, sobrenomes, números de documentos, placas de carros, números de telefones, datas que possam ser relacionadas com o usuário ou palavras constantes em dicionários;
e) Alterar periodicamente suas senhas; (60 Dias) *O não cumprimento deste tópico acarretará o bloqueio dos acessos...
f) Certificar a procedência do sítio e a utilização de conexões seguras (criptografadas) ao realizar transações via web;
g) Verificar se o certificado do sítio ao qual se deseja acessar, esta integro e corresponde realmente aquele sítio, observando ainda, se o mesmo está dentro do prazo de validade;
h) Certificar que o endereço apresentado no navegador corresponde ao sítio que realmente se quer acessar, antes de realizar qualquer ação ou transação;
i) Digitar no navegador o endereço desejado e não utilizar links como recurso para acessar um outro endereço destino;
j) Não abrir arquivos ou executar programas anexados a e-mails, sem antes verifica-los com um antivírus;
k) Não utilizar o formato executável em arquivos compactados, pois estes tipos são propícios à propagação de vírus.

12.3 Recomendações sobre atividades permitidas

Recomenda-se:

a) Utilizar programas de computador licenciados, de acordo com as disposições específicas previstas em contrato. A instalação de programas e sistemas homologados é atribuição da administração de sistemas e TI;
b) Criar, transmitir, distribuir, disponibilizar e armazenar documentos, desde que respeite às leis e regulamentações, notadamente àqueles referentes aos crimes informáticos, ética, decência, pornografia envolvendo crianças, honra e imagem de pessoas ou empresas, vida privada e intimidade;
c) Fazer cópia de documentos e ou programas de computador a fim de salvaguardá-los, respeitada a legislação que rege a salvaguarda de dados, informações, documentos e materiais sigilosos.

12.4 Recomendações sobre atividades não permitidas

Recomenda-se não fazer:

a) Introduzir códigos maliciosos nos sistemas de TI;
b) Revelar códigos de identificação, autenticação e autorização de uso pessoal (conta, senhas, chaves privadas etc.) ou permitir o uso por terceiros de recursos autorizados por intermédio desses códigos;
c) Divulgar ou comercializar produtos, itens ou serviços a partir de qualquer recurso dos sistemas de TI;
d) Tentar interferir um serviço, sobrecarregá-lo ou, ainda, desativá-lo, inclusive aderir ou cooperar com ataques de negação de serviços internos ou externos;
e) Alterar registro de evento dos sistemas de TI;
f) Modificar cabeçalho de qualquer protocolo de comunicação de dados;
g) Obter acesso não autorizado, ou acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades nos sistemas de TI;
h) Monitorar ou interceptar o tráfego de dados nos sistemas de TI, sem a autorização de autoridade competente;
i) Violar medida de segurança ou de autenticação, sem autorização de autoridade competente;
j) Fornecer informações a terceiros, sobre clientes ou serviços disponibilizados nos sistemas de TI, exceto os de natureza pública ou mediante autorização de autoridade competente;
k) Fornecer dados classificados de acordo com a legislação vigente, sem autorização de autoridade competente;
l) Armazenamento ou uso de jogos em computador;
m) Uso de recurso informacional da entidade pública para fins pessoais, incluindo entre estes o comércio, venda de produtos ou engajamento em atividades comerciais de qualquer natureza;

n) Uso de aplicativos não homologados.
o) O uso de pen-drives genéricos são banidos da organização, permitidos apenas pen-drives tratados conforme política de uso de criptografia desse hardwares.

12.5 Assinatura Eletrônica E-mail.

Desenvolvimento de Termo

12.6 Coleta de Dados em Formulários Eletrônicos

Para coletar e processar dados sensíveis nos formulários de inscrição, A ABAPA necessita do consentimento expresso dos usuários, ou seja, o usuário ou participante deve conhecer e concordar livremente com a coleta, utilização ou compartilhamento dos seus dados.

Assim sendo, fica definido o meio de coleta eletrônica de dados através da plataforma **Microsoft Forms,** pelo link https://forms.office.com/ onde seu acesso é definido através do e-mail corporativo @abapa.com.br.

Fica definido a plataforma Google Forms https://www.google.com/intl/pt-BR/forms/about/ como ferramenta complementar para coleta de dados, porém seu uso só será permitido com acesso supervisionado pela Governança Local e T.I.

Qualquer outro meio que não mencionado que venha ser utilizado para coleta de dados é caracterizado como quebra dessa política.

12.5.1 Para que o procedimento seja efetivo é fundamental que possua no campo do formulário o termo, assim o usuário pode decidir fornecer ou não essas informações.

Para isso, ao adicionar o campo customizado no qual você coletará algum dado sensível, é necessário deixar desmarcada a opção “Campo de preenchimento obrigatório”.

Além do consentimento, é muito importante incluir uma “Declaração de Privacidade” no “Termo de Responsabilidade” da coleta. Esse documento é fundamental para aumentar a transparência sobre a utilização dos dados pessoais dos compradores ou participantes, principalmente dados sensíveis.

Indique para quais finalidades você está coletando esses dados.

Informe se você compartilha essas informações com terceiros (ex.: patrocinadores, fornecedores, parceiros comerciais, agências de marketing, etc.), assim como o nome deles e o motivo desse compartilhamento.

Ofereça meios para que os usuários/candidato entrem em contato com você em caso de dúvidas.

Existem outras informações que também são importantes incluir no seu termo, como por exemplo: período de armazenamento dos dados, medidas de segurança adotados, meios para exercício de direitos, link para a política de privacidade de parceiros, entre outros.

Lembre-se que quanto mais transparência você oferece na sua Declaração de Privacidade, mais confiança você passa para os compradores ou participantes, e isso é muito valioso para o sucesso dos seus eventos.

12.7 Recomendações específicas

1.7.10 Proteção de equipamentos

Todos os equipamentos de processamento de informação (servidores, computadores, impressoras, laptops, notebooks, hubs, switches, rádio, palmtops, etc.) devem ser ligados em rede elétrica aterrada, estabilizada, e de acordo com as especificações do fabricante do equipamento.

Todos os equipamentos de processamento de informação devem ser mantidos em ambiente protegidos de fogo, água, fumaça, poeira e vibração, e devem ser mantidos em temperatura adequada ao seu funcionamento, conforme as especificações do fabricante do equipamento.

12.8 Mesa e tela limpa

Todos os colaboradores deverão obedecer às regras de limpeza e organização do ambiente de trabalho a fim de não expor desnecessariamente Informações classificadas.

Para evitar exposição desnecessária de informações, recomenda-se que papéis e mídias de computador não sejam deixados sobre a mesa de trabalho.

Recomenda-se que os colaboradores tenham cuidado com a exposição de informações sensíveis em telas de computadores em ambientes de circulação ou públicos.

Recomenda-se que informações sensíveis, quando impressas, sejam retiradas imediatamente da impressora.

Proibido realizar refeições próximos os equipamentos de informática.

12.9 Trabalho remoto

O acesso aos recursos e informações da **ABAPA** a partir da Internet pode ser feito, mas com autorização prévia do gerente da área solicitante e do departamento de TI, e a partir de computadores exclusivos da empresa por meio do software VPN Firewall Shophos, mediante a disponibilização do recurso de T.I.

O acesso remoto de terceiros a partir de computadores particulares deve ser realizado apenas mediante autorização do coordenador da área solicitante e do departamento de TI. Os contratos de terceiros devem prever a possibilidade de auditoria por parte da **ABAPA** para garantir o cumprimento dos requisitos de segurança.

Recomenda-se evitar o trabalho remoto em áreas públicas, como shoppings centers, aeroportos, aviões, entre outros, para evitar a exposição das informações e ativos corporativos a incidentes de segurança.

O trabalho remoto deve ser realizado no horário do expediente. O acesso fora do horário deve ser autorizado previamente pelo gerente do colaborador.

Colaboradores em férias ou afastados por qualquer outro motivo não poderão realizar trabalho remoto, nem utilizar recursos de TI da **ABAPA**.

12.10 Uso de correio eletrônico

O correio eletrônico da **ABAPA** , assim como todas as plataformas de comunicação utilizadas na empresa, são ferramentas de trabalho, não devendo ser utilizado para outros fins.

As informações contidas nas mensagens eletrônicas são de propriedade da **ABAPA**, podendo ser monitoradas a qualquer tempo, sem aviso ou notificação prévia, para fins de auditoria de conformidade às normas internas, regulamentações ou boas práticas aplicadas ao negócio da empresa.

É expressamente proibido o envio de Informações classificadas como “INTERNAS” e “CONFIDENCIAIS” para endereços de e-mail para endereços de outros domínios além da

ABAPA, exceto para terceiros (clientes ou fornecedores) diretamente envolvidos no respectivo assunto da mensagem.

As informações classificadas como “CONFIDENCIAIS” não devem ser armazenadas ou transmitidas por e-mail simples. Para isso, é obrigatório o uso de criptografia forte adicional para proteção do conteúdo da mensagem e seus anexos, por meio de solicitação à área de Segurança de Informação e autorização do superior imediato.

Quando um colaborador da **ABAPA** for desligado, deverão ser observados os seguintes procedimentos em relação ao seu e-mail corporativo: a) O colaborador, independentemente de seu cargo, deverá ser informado de que seu e-mail corporativo foi suspenso e que o colaborador poderá, desde que acompanhado por um outro colaborador da empresa designado para essa tarefa, retirar eventual e-mail pessoal e informações pessoais constantes em sua caixa de e-mails corporativa e/ou arquivos digitais e físicos.

12.11 Outros meios de comunicação eletrônica

A comunicação eletrônica dos colaboradores da **ABAPA** com o mundo externo está restrita a e-mail coorporativo, telefones coorporativos, aplicativos de mensagens registros pela empresa.

Ferramentas como Skype, Google Talk, Google Docs, Skydrive, P2P (Peer-to-Peer), e similares são expressamente proibidas. Exceções serão analisadas, mediante autorização da gerência da área solicitante e do departamento de TI, mas apenas para uso corporativo. O serviço de mensagem instantânea interno é permitido e reuniões deverão ser feias realizadas através do ZOOM e Teams, esses meios de comunicação podem ser monitorados.

.

12.12 Senhas de acesso

A senha de acesso aos recursos computacionais da **ABAPA** é de inteira responsabilidade do colaborador, que não deverá, em hipótese alguma, compartilhar ou emprestar a outros colaboradores e terceiros.

Os usuários deverão utilizar senhas “fortes”, misturando letras e números, em todos os sistemas corporativos e o tamanho mínimo recomendado para as senhas é de 9 (nove) caracteres.

Informações classificadas como SECRETAS deverão obrigatoriamente utilizar uma sequência longa de pelo menos 16 caracteres, ou optar pela utilização de uma chave

criptográfica de pelo menos 1024 bits (utilizando-se sempre uma senha adicional para a proteção da chave criptográfica).

Toda ação feita, dentro ou fora do ambiente computacional da **ABAPA** será de responsabilidade do colaborador associado às credenciais de acesso associadas às ações.

12.13 Acesso e uso da internet

A **ABAPA** poderá permitir acesso à Internet e a navegação em sites de conteúdo, sempre de acordo com a sua política de Segurança da Informação e bloqueios de sites classificados como inseguros ou não confiáveis.

É explicitamente proibido a transferência de arquivos por meio de quaisquer protocolos, aplicativo ou ferramenta que não forem previamente e explicitamente aprovados pela área de Segurança da Informação da **ABAPA**.

Essa aprovação é uma análise de segurança da ferramenta e do fornecedor do produto, a fim de garantir que somente ferramentas e fabricantes que possuam alta maturidade em Segurança da Informação, proteção de dados e políticas claras de privacidade, sejam incorporados à lista de ferramentas e fornecedores aprovados. Isso evita a herança de vulnerabilidades por meio de ferramentas não seguras e não testadas, assim como parcerias com fornecedores que possam não seguir as boas práticas de Segurança da Informação. Da mesma forma, não será permitido o download de materiais protegidos por direitos autorais ou a instalação de softwares não homologados pela área de Segurança da Informação. O colaborador deve consultar o departamento de TI antes de fazer o download de qualquer software de terceiro.

12.14 Software, apps e plug-ins

Não é permitido a instalação de softwares não aprovados pela área de TI e Segurança de Informação em quaisquer dispositivos que acessam os sistemas de Informação da **ABAPA** que inclui: computadores, notebooks e dispositivos portáteis como tablets e celulares. Inclusive software, aplicativos, plug-ins pagos ou gratuitos.

A área de TI devem possuir um portfólio de ferramentas e aplicativos para atender as demandas do negócio incluindo ferramentas de produtividade e afins.

A maioria dessas ferramentas já são previamente instaladas em todos os dispositivos corporativos.

12.15 Postura geral de privacidade

Todos os acessos aos sistemas internos devem ter como justificativa um propósito real de negócio.

É expressamente proibido o acesso a quaisquer Informações de clientes, colaboradores ou qualquer registro nos sistemas de Informação da **ABAPA** sem um propósito claro de negócio, e ligado diretamente ao exercício das funções atribuídas na relação de trabalho entre o colaborador e a empresa.

É expressamente proibido o acesso a dados de clientes por mera curiosidade, por exemplo: acessar contas de celebridades, pessoas públicas, parentes, amigos ou qualquer outro cliente sem que haja um propósito de negócio e principalmente, um chamado relacionado ao caso; caso precise resolver algum problema na sua própria conta, como alterar uma Informação de cadastro, abra um chamado e peça que um colega faça a alteração para você.

13. MONITORAÇÃO

A **ABAPA** se reserva ao direito de monitorar todas as atividades feitas pelos seus colaboradores em seus sistemas de informação para garantir o cumprimento desta e outras políticas da empresa.

14. TREINAMENTO E CONSCIENTIZAÇÃO

A **ABAPA** promove a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação para fortalecer a cultura de Segurança da Informação.

Periodicamente, são disponibilizadas campanhas de conscientização ou treinamentos que podem ser presenciais ou on-line, relacionados a confidencialidade, integridade e disponibilidade da informação.

Todos os colaboradores devem receber treinamento e conscientização em Segurança da Informação e na Política de Segurança da Informação, especialmente os novos colaboradores.

15. VIOLAÇÃO

É política da **ABAPA** atua de forma justa e proporcional, considerando as ações a serem tomadas para informar as partes afetadas com relação a violações de dados pessoais.

A violação desta Política de Segurança da Informação poderá acarretar sanções administrativas e/ou legais, sem prejuízo da rescisão do contrato de trabalho e/ou qualquer outro contrato de relacionamento de prestação de serviço entre o colaborador, associado, consultor e/ou sócio, assim como qualquer entidade com relação contratual direta ou indireta com a **ABAPA. Consultar regimento interno deve constar a citação das violações.**

16. ATUALIZAÇÃO DA POLÍTICA

A **ABAPA** assume o compromisso de revisitar a presente Política de Segurança da Informação periodicamente e, ao seu critério, promover modificações que atualizem suas disposições de modo a reforçar o compromisso permanente da empresa com a privacidade e a proteção de dados pessoais, sendo comunicadas todas as alterações realizadas oportunamente pelos canais oficias da empresa.

17. ENCARREGADO DE PROTEÇÃO DE DADOS

A **ABAPA** destaca que, se após a leitura desta Política de Segurança da Informação, ainda restar dúvidas ao titular de dados pessoais ou caso esse precise comunicar qualquer incidente envolvendo seus dados pessoais, o contato deverá ser realizado com o (DPO), por meio dos seguintes canais de comunicação:

18. ATUALIZAÇÃO DA POLÍTICA DE PROTEÇÃO DE DADOS

A política de proteção de dados está em constante aperfeiçoamento, podendo ser alterada frente às exigências ou necessidades advindas da lei, regulamentos, provimentos, decisões judiciais, pareceres, ou propostas de segurança da informação.

Sugerimos que a leitura da política de proteção de dados seja feita periodicamente, a fim de se manter atualizado e ciente da segurança das informações.

Atualização	Responsável	Autor	Resumo de mudanças
11/04/2022	Núcleo de Proteção de Dados do Oeste da Bahia.	Reinaldo Almeida – Encarregado de Dados	Primeira Versão
13/05/2022	Núcleo de Proteção de Dados do Oeste da Bahia.	Pacheco & Queiroz Advogados Associados	Atualização, conferencia e conversão em PDF.

19.MAIORES INFORMAÇÕES

Se após a leitura da política de proteção de dados ainda restar dúvidas ao usuário ou se precisar comunicar qualquer incidente envolvendo dados pessoais, o contato deverá ser realizado através do Encarregado de dados (DPO), via os canais de comunicação.

ENCARREGADO DE DADOS EXTERNO (DPO AS A SERVICE):
Núcleo de Proteção de Dados do Oeste Baiano – NPDO
Vinculado mediante Contrato de Prestação de Serviços
Rua Coronel Magno, 616, escritório 202, Bairro Centro,
Barreiras – BA, CEP 47.800-154
Horário de atendimento: Seg. a Sex. das 08h00m às 17h00m
Telefone e WhatsApp: (77) 99861-0707
E-mail: seguranca@npdob.com.br