POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E GESTÃO DE ATIVOS

1. Introdução – Política de Segurança da Informação e Gestão de Ativos

1.1. Objetivo

1.1.1. A presente Política de Segurança da Informação e Gestão de Ativos ("Política") tem como propósito estabelecer diretrizes e normas sobre segurança da informação e gestão de ativos informacionais do /asbz, além de definir os papéis e responsabilidades de seus(as) colaboradores(as), terceiros e prestadores de serviços, visando proteger as informações do /asbz, dos seus clientes e do público em geral.

1.1.2. Esta Política deve ser lida em conjunto com as normas adicionais abaixo, sendo que, em caso de divergência entre qualquer uma delas e esta Política, prevalecerão as disposições de conteúdo mais específico.

- Código de Conduta e Ética

- Plano de Continuidade de Negócio

- Política de Privacidade de Website

1.2. Conceito

1.2.1. A informação é um ativo que possui grande valor para o /asbz, devendo ser adequadamente utilizada e protegida por seus(as) colaboradores(as), parceiros e prestadores de serviços. A adoção de políticas, normas e procedimentos que visem garantir a segurança das informações corporativas deve ser prioridade constante da organização, para que sejam reduzidos os riscos de falhas, danos e/ou prejuízos que possam comprometer a imagem e os objetivos do /asbz.

1.2.2. A informação pode ser manipulada de diversas formas: por meio de arquivos eletrônicos, Internet, banco de dados, mensagens eletrônicas, em meio impresso, verbalmente, em mídias removíveis, e dentre outros meios presentes em nosso cotidiano como, por exemplo, o uso de celulares, *notebooks* corporativos e/ou pessoais;

1.2.3. A segurança da informação é aqui caracterizada pela preservação dos seguintes princípios:

1.2.3.1. **Confidencialidade:** Garantia de que o acesso à informação seja obtido e concedido somente por pessoas autorizadas;

1.2.3.2. **Disponibilidade:** Garantia de que os(as) colaboradores(as), terceiros e

prestadores de serviços autorizados obtenham acesso à informação (e aos ativos correspondentes) sempre que necessário, limitado ao que for de fato essencial para a finalidade em questão; e

1.2.3.3. **Integridade:** Garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais; ou seja, somente alterações, supressões e adições autorizadas pelo /asbz devem ser realizadas nas informações.

1.2.4. Para assegurar esses conceitos, a informação deve ser adequadamente gerenciada e protegida contra fraude, espionagem, perda não intencional, acidentes e outras ameaças provenientes de fragilidades em sistemas, processos e pessoas.

1.3. Aplicabilidade

1.3.1. Aplica-se a todos os(as) colaboradores(as), permanentes ou temporários, bem como a terceiros e prestadores de serviços, que acessem as informações pertencentes ao /asbz, os quais devem ler, conhecer e agir conforme os termos e condições desta Política.

1.3.2. A Política aplica-se, também, a todos os locais a partir dos quais os sistemas do /asbz possam ser acessados (incluindo o uso doméstico). Terceiros que tenham acessos aos sistemas do /asbz, por meio de *links*, devem demonstrar que possuem uma política de segurança da informação que esteja em conformidade com os requisitos de segurança adotados pelo /asbz. Uma cópia de qualquer política de segurança de terceiros será mantida com o contrato ou acordo celebrado.

1.3.3. Todo e qualquer Usuário de recursos computadorizados do /asbz tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de TI.

1.4. Política

1.4.1. O /asbz compromete-se a:

- Proteger a confidencialidade, integridade e disponibilidade de todos os dados que ele mantém em seus sistemas. Isso inclui a proteção de qualquer dispositivo pertencente ao /asbz que possa transportar ou acessar dados, além de proteger cópias físicas dos dados em papel sempre que possível (por exemplo, normas sobre manuseio, armazenamento e eliminação de documentos);
- Cumprir as obrigações legais e contratuais;
- Proteger os direitos de propriedade intelectual do /asbz;
- Produzir, manter e testar planos de continuidade de negócios;
- Proibir o uso não autorizado das informações e sistemas do /asbz;

- Comunicar e difundir esta Política a todas as pessoas que tratam dados do escritório;
- Fornecer treinamento em segurança da informação e proteção de Dados Pessoais aos(às) colaboradores(as) do escritório; e
- Conduzir internamente, de forma adequada, todos os procedimentos para sanar violações à segurança da informação, reais ou suspeitas, e, quando necessário, reportá-las aos órgãos competentes, incluindo, sem limitação, a Autoridade Nacional de Proteção de Dados ("ANPD").

1.5. Avaliação de riscos e classificação de informações

1.5.1. O grau de controle de segurança necessário depende da sensibilidade ou criticidade das informações. A primeira etapa na determinação do nível apropriado de segurança é, portanto, um processo de avaliação de riscos, a fim de identificar e classificar a natureza das informações mantidas, as consequências adversas das violações de segurança e a probabilidade dessas consequências ocorrerem;

1.5.2. A avaliação de risco deve identificar os ativos de informações do /asbz; definir a propriedade desses ativos; e classificá-los de acordo com sua sensibilidade e/ou criticidade para o /asbz como um todo. Ao avaliar o risco, o /asbz deve considerar o valor do ativo, as ameaças a esse ativo e sua vulnerabilidade;

1.5.3. Onde apropriado, os ativos de informação devem ser rotulados e manipulados de acordo com a criticidade e a sensibilidade;

1.5.4. As avaliações de risco à segurança da informação devem ser revisadas periodicamente e realizadas conforme necessário durante a entrega e manutenção operacional da infraestrutura, sistemas e processos do /asbz;

1.5.5. Os Dados Pessoais devem ser tratados de acordo com as disposições da LGPD, eventuais diretrizes de autoridades competentes, incluindo, sem limitação, a ANPD, e de acordo com esta Política;

1.5.6. A LGPD exige que sejam tomadas as medidas técnicas e organizacionais apropriadas contra o tratamento não autorizado ou ilegal de Dados Pessoais, bem como contra a perda/destruição acidental ou danos a Dados Pessoais; e

1.5.7. Um nível mais alto de segurança deve ser fornecido, quando necessário, para os chamados Dados Pessoais sensíveis e de menores de idade, definidos pela LGPD como aqueles relacionados a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, e dados genéticos ou biométricos, quando vinculado a uma pessoa natural.

2. Glossário

2.1. Segurança da Informação

2.1.1. Consiste, segundo o contexto desta Política, no conjunto de diretrizes e boas práticas relacionadas ao uso e confidencialidade de informações, Dados Pessoais e processos sob a gestão de todos e quaisquer colaboradores(as), terceiros e prestadores de serviço. Ou seja, trata-se de todos os documentos, padrões ou manuais que determinam as ações para garantir a segurança da informação.

2.2. Ativo da Informação

2.2.1. Ativo de informação é qualquer elemento que sustenta um ou mais processos de negócio de uma unidade ou área de negócio, ou seja, tudo aquilo que tem valor para o escritório. A ISO 27001 exige que todos os ativos relevantes sejam identificados e inventariados. Quando o assunto é segurança da informação, por "inventário de ativos" deve-se compreender um conjunto mais abrangente de ativos, que contempla sistemas, pessoas, ambientes físicos, entre outros.

2.2.2. Seguem abaixo alguns exemplos de ativos:

Usuários	Computadores	Discos
Impressoras	Mídias móveis	Sistemas
Banco de dados	Servidores	Switches de rede
Links	Documentos	Acordos
Contratos	Scanners	Administradores

2.3. Ameaça

2.3.1. Causa potencial de um incidente, que pode vir a prejudicar o /asbz.

2.4. Incidente de Segurança da Informação

2.4.1. Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de informação, que ocasione, de maneira acidental ou ilegal, à destruição, perda, alteração, acesso ou aquisição não autorizada, divulgação, utilização abusiva ou acesso a informações e Dados Pessoais não criptografados, transmitidos, armazenados ou de algum modo tratado pelo /asbz.

2.5. Usuários

2.5.1. Advogados, estagiários, aprendizes, trabalhadores(as) com vínculo empregatício, de qualquer área, ou terceiros alocados na prestação de serviços, independentemente do regime jurídico a que estejam submetidos, assim como outros indivíduos, colaboradores(as), ou organizações devidamente autorizadas a utilizar manipular qualquer ativo de informação do /asbz para o desempenho de suas atividades profissionais.

2.6. Dados Pessoais

2.6.1. Toda e qualquer informação que diga respeito a um indivíduo, identificado ou identificável, incluindo, mas não se limitando a, nome, documentos de identificação, números de telefones, endereços de e-mail, endereço de postagem, dados bancários e financeiros, data de nascimento, gênero, filiação, informações demográficas, dentre outras.

2.7. Informações Confidenciais

2.7.1. Inclui, mas não se limita a, informação – seja qual for a forma de armazenagem – relacionada ao /asbz e aos seus negócios, informação relacionada a clientes ou clientes em potencial, informação sujeita a restrição de divulgação, informação sujeita a direito de propriedade ou segredo comercial, informação que não esteja prontamente disponível ao público e, ainda, toda e qualquer informação que um colaborador do /asbz saiba ou deveria saber ser considerada sensível pelo /asbz, seus clientes e clientes em potencial como materiais confidenciais. São exemplos: documentos, contratos, gráficos, imagens, desenhos, designs, *know-how,* segredos comerciais, informações comerciais, técnicas, administrativas, estratégicas, de marketing, informações financeiras e outros dados.

2.7.2. Caso o Usuário tenha dúvida ao avaliar se uma informação ou dado é ou não confidencial, deve tratá-lo como confidencial.

2.8. Encarregado pelo Tratamento de Dados (DPO)

2.8.1. Equipe ou indivíduo responsável dentro do /asbz para atuar como canal de comunicação entre o escritório, os titulares de Dados Pessoais e a ANPD. Além disso, cabe ao DPO auxiliar o escritório no cumprimento de suas obrigações legais referentes à privacidade e a proteção de Dados Pessoais.

2.9. Autoridade Nacional de Proteção de Dados (ANPD)

2.9.1. Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

3. Atribuições e responsabilidades

3.1. Grupo de Trabalho de Segurança da Informação

3.1.1. Fica constituído o Grupo de Trabalho de Segurança da Informação, a ser indicado pelo(a) Diretor(a) de Inovação do /asbz, conforme as demandas necessárias;

3.1.2. O grupo tem a responsabilidade de analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação e à gestão dos ativos do /asbz;

3.1.3. Garantir a disponibilidade dos recursos necessários para uma efetiva gestão de Segurança da Informação e dos ativos;

3.1.4. Garantir que as atividades de segurança da informação sejam executadas em conformidade com esta Política;

3.1.5. Promover a divulgação da Política e tomar as ações necessárias para disseminar uma cultura de segurança da informação e proteção de Dados Pessoais no ambiente do /asbz;

3.1.6. Analisar e apurar incidentes referentes à Política; e

3.1.7. Decidir sobre a aplicação de sanções aos incidentes identificados e analisados.

3.2. Departamento de Tecnologia da Informação (TI)

O Departamento de Tecnologia da Informação tem como suas responsabilidades:

3.2.1. Apoiar o Grupo de Trabalho de Segurança da Informação do /asbz em suas deliberações;

3.2.2. Conduzir a gestão e operação da Segurança da Informação, bem como a gestão dos ativos, tendo como base esta Política e demais normas e procedimentos do /asbz;

3.2.3. Prover todas as informações de gestão de Segurança da Informação e, quando for o caso, dos ativos, que sejam solicitadas pelo Grupo de Trabalho de Segurança da Informação ou pela Diretoria Executiva;

3.2.4. Elaborar e propor ao Grupo de Trabalho de Segurança da Informação do /asbz as normas e procedimentos de segurança da informação e gestão de ativos, necessários para se fazer cumprir a Política;

3.2.5. Antes de conceder acesso às informações do /asbz, exigir a assinatura de acordo de confidencialidade dos(as) Usuários(as) que não estejam cobertos por um contrato existente ou obrigação legal ou regulatória, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais;

3.2.6. Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;

3.2.7. Tomar as ações cabíveis para se fazer cumprir os termos desta Política;

3.2.8. Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado aos casos identificados;

3.2.9. Garantir que as atividades de segurança da informação sejam executadas em conformidade com a presente Política; e

3.2.10. Conduzir treinamentos aos Usuários e tomar as demais medidas cabíveis para a divulgação da PSI e assimilação de todos os seus conceitos e obrigações dos Usuários.

3.3. Usuários(as)

Os(As) Usuários(as) são responsáveis por:

3.3.1. Ler, compreender e cumprir integralmente os termos da Política, bem como das demais normas e procedimentos adjacentes;

3.3.2. Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política, suas normas e procedimentos ao Grupo de Trabalho de Segurança da Informação do /asbz;

3.3.3. Comunicar ao Diretor(a) de Inovação do /asbz qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações, dos recursos computacionais e dos ativos do /asbz;

3.3.4. Participar de todos os treinamentos disponibilizados pelo Grupo de Trabalho de Segurança da Informação a respeito de Segurança da Informação; e

3.3.5. Responder pelo não cumprimento da Política, normas e procedimentos de segurança, conforme definido no item sanções e punições.

4. Diretrizes Gerais

4.1. Aspectos Gerais

4.1.1. A presente Política é parte integrante do contrato de trabalho verbal ou tácito, escrito ou expresso dos(as) Usuários(as), para todos os fins de direito juntamente com o kit admissional fornecido pelo departamento de Gestão de Pessoas;

4.1.2. Essa Política dá ciência a cada usuário(a) de que os ambientes, sistemas, dispositivos, servidores e redes do /asbz poderão ser monitorados e gravados, e que os registros assim obtidos poderão ser utilizados para detecção de violações desta Política e demais normas de segurança da informação, podendo estes servir de evidência para a aplicação de medidas disciplinares, processos administrativos e/ou judiciais;

4.1.3. Uma atitude engajada e proativa no que diz respeito à proteção das informações do /asbz deve ser prioridade constante de todos(as) os(as) Usuários(as) e áreas de negócio, reduzindo-se os riscos de falhas, os danos e/ou prejuízos que possam comprometer a imagem e os objetivos organizacionais;

4.1.4. As informações corporativas devem ser manuseadas de acordo com as leis vigentes e normas internas e utilizadas apenas para a finalidade para a qual foi coletada, evitando seu mau uso e/ou exposição indevida; e

4.1.5. É proibido que os(as) Usuários(as) façam o uso de dados da empresa para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou normas.

4.2. Acesso à Informação e aos sistemas de informação

4.2.1. As informações (em formato físico ou lógico) e os ambientes tecnológicos corporativos utilizados pelos(as) Usuários(as) são de exclusiva propriedade do /asbz, não podendo ser interpretados como de uso pessoal;

4.2.2. O acesso às informações do /asbz deve ser restrito a Usuários(as) autorizados e deve ser protegido por controles físicos e/ou lógicos práticos adequados;

4.2.3. As permissões de acesso aos sistemas e plataformas do /asbz serão concedidas pelo Departamento de Tecnologia da Informação;

4.2.4. As permissões de acesso dos(as) Usuários(as) que, para desempenho de suas atividades, necessitem de acesso aos sistemas do /asbz devem ser concedidas apenas durante o prazo de seu contrato;

4.2.5. O acesso a ativos de informações físicas – por exemplo, documentos impressos em papel e mídia contendo informações – será regido de acordo com os princípios acima, naquilo que for aplicável;

4.2.6. Procedimentos próprios devem estar em vigor para garantir que todos(as) os(as) Usuários(as) tenham informações e permissões de acesso físico concedidas com rapidez ao ingressar no /asbz, sejam revogadas ao deixar a organização e atualizadas quando houver mudança de função. Aqueles que forem desligados ou tiverem seu contrato encerrado também serão obrigados a devolver todos os ativos do /asbz que estejam em sua posse após a rescisão do contrato;

4.2.7. Os privilégios de administrador de domínio – aqueles que são capazes de substituir os controles de sistemas e aplicativos em vários dispositivos em todo o /asbz – devem ser restritos às pessoas autorizadas a executar apenas a administração de sistemas. Tais privilégios devem ser autorizados pelo Departamento de Tecnologia da Informação, uma vez analisadas e feitas avaliações de risco apropriadas quanto à validade dos requisitos e aos níveis de habilidade daqueles que solicitam privilégios aumentados;

4.2.8. Todos os fornecedores ou contratados que tratam informações do /asbz devem fornecer ao /asbz garantias de que possuem controles compatíveis com os preceitos da LGPD, bem como com aqueles adotados pelo próprio /asbz; e

4.2.9. Nos casos em que os dados tratados pelo fornecedor ou contratado forem sensíveis (conforme definido pelo LGPD), uma avaliação de segurança de terceiros (*vendor assessment*) deve ser preenchida pelo fornecedor.

4.3. Uso de dispositivo de armazenamento removível e equipamento de computador pessoal

4.3.1. O /asbz reconhece que pode haver ocasiões em que os Usuários(as) precisem usar dispositivos de armazenamento removível fornecidos pelo /asbz para acessar informações (incluindo Dados Pessoais). O /asbz deve garantir que todos os dispositivos fornecidos sejam totalmente criptografados e que os(as) Usuários(as) estejam cientes dessa política;

4.3.2. O /asbz reconhece que pode haver ocasiões em que os Usuários(as) precisem utilizar seu próprio dispositivo para acessar informações (incluindo Dados Pessoais e emails). Os(As) Usuários(as) devem garantir que tais dispositivos sejam protegidos por fatores de autenticação apropriados e antivírus. O Departamento de Tecnologia da Informação ou o(a) Diretor(a) de Inovação do /asbz poderá revogar o acesso aos sistemas ou informações do /asbz em dispositivos pessoais onde os dados contidos/transmitidos são considerados sensíveis e o dispositivo pessoal não é adequado.

4.3.3. É estabelecido aos(às) Usuários(as) que:

- Os equipamentos de computação de propriedade privada usados para acessar as informações do /asbz ou se conectar à rede do /asbz devem ser protegidos por senha, possuir antivírus atualizado instalado, bem como todas as atualizações relevantes do sistema operacional e todos os programas de terceiros que o Departamento de Tecnologia da Informação julgar necessário;
- O uso de dispositivos pessoais para acessar e-mails é permitido. Recomenda-se que os(as) Usuários(as) procurem orientação do Departamento de Tecnologia da Informação para garantir que a configuração das conexões de e-mail seja segura, os dispositivos sejam protegidos com bloqueio de chave/senha/biometria e, quando apropriado ou viável, criptografia de dispositivo; e
- O /asbz reserva-se o direito de interromper a transmissão ou o acesso a qualquer um dos dados que possui, se esta Política não for seguida.

4.3.4. O /asbz reserva-se o direito de desconectar o dispositivo de sua rede corporativa e desabilitar seus serviços sem prévia notificação, caso constatado eventual incidente de segurança (vírus, violação de dados, dentre outros) ou em caso de violação desta Política e demais normas de segurança da informação ou em situações deliberadas pelo(a) Diretor(a) de Inovação do /asbz; e

4.3.5. No caso de incidentes de segurança da informação envolvendo dispositivos que contenham ativos de informação do /asbz, os(as) Usuários(as) deverão imediatamente comunicar o ocorrido por meio do e-mail do(a) Diretor(a) de Inovação do /asbz e incidentes@asbz.com.br.

4.4. Monitoramento de computadores, e-mail e Internet

4.4.1. O e-mail dos(as) Usuários(as) do /asbz não é rotineiramente lido ou monitorado. Entretanto, para garantir a segurança, confidencialidade, disponibilidade e integridade dos sistemas e ativos de TI do /asbz, sob determinadas circunstâncias, a fim de verificar situações de fraudes e de incidentes de segurança da informação, membros autorizados do Departamento de Tecnologia da Informação, ou outro pessoal autorizado, poderão acessar os computadores do /asbz, e-mails e sistemas de internet – incluindo plataformas digitais online como nuvem ou outros sistemas de gravação, banco de dados e *backups*; e

4.4.2. O /asbz poderá investigar violações à lei ou normas e políticas internas da própria empresa, o que pode envolver o acesso ao computador e aos registros eletrônicos do colaborador. Tal investigação poderá ocorrer mediante suspeita de má conduta ou falta grave incorrida pelo colaborador, e será conduzida de acordo com as disposições do Código de Conduta e Ética.

4.5. Monitoramento por câmeras de segurança

4.5.1. Para reforçar a segurança de seus(as) colaboradores(as) e dos visitantes às suas instalações, o /asbz opera câmeras de segurança em todas as suas dependências. O sistema de vigilância é contínuo e permanente;

4.5.2. As câmeras não são utilizadas para vigilância de pessoas específicas, mas as imagens gravadas podem ser acessadas e usadas para monitoramento das atividades relacionadas ao /asbz, inclusive como suporte em investigações internas ou promovidas pelas autoridades competentes; e

4.5.3. Câmeras em geral, incluindo de telefones celulares próprios, não devem ser usadas para gravação de imagens de operações do /asbz ou de nenhum indivíduo, sem seu prévio consentimento.

4.6. Mesa limpa/tela bloqueada

4.6.1. Fora do horário normal de trabalho, todas as informações confidenciais, marcadas como tal ou não, devem ser protegidas; isso pode incluir dentro de um armário próprio trancado ou em uma mesa com gavetas trancadas. Durante o horário normal de expediente, essas informações devem ser ocultadas ou protegidas caso não haja vigilância das mesas ou em se tratando de um ambiente *open space*;

4.6.2. As informações confidenciais impressas que serão descartadas oportunamente devem ser colocadas em um compartimento próprio para descarte de materiais confidenciais assim que possível, ou mantidas em segurança até o momento do descarte;

4.6.3. Os documentos devem ser retirados imediatamente de impressoras e fotocopiadoras, após sua utilização;

4.6.4. Os computadores de mesa devem ser desconectados ou bloqueados automaticamente após 5 minutos (a menos que seja necessário permanecer ativados para fins operacionais), para garantir que os sistemas de computadores autônomos não se tornem um meio potencial de obter acesso não autorizado à rede;

4.6.5. Os responsáveis pelas reuniões devem garantir que nenhuma informação confidencial seja deixada na sala ao final da reunião, até mesmo documentos jogados em cestos de lixo; e

4.6.6. O /asbz deve garantir que os(as) Usuários(as) tenham instalações de armazenamento adequadas e suficientes para que possam cumprir com esta Política.

4.7. Segurança de mídia física

4.7.1. Os(As) responsáveis pelas informações devem garantir que qualquer mídia física (por exemplo, papel, CD-ROMs, HDs) usada para armazenar informações que

contenham Dados Pessoais seja protegida, a fim de impedir o acesso não autorizado de terceiros;

4.7.2. A segurança física de tais informações deve se dar em forma de armários com chave ou outros compartimentos não facilmente transportáveis, com chaves ou códigos de combinação acessíveis apenas às pessoas autorizadas. Quando os armários ou compartimentos de armazenamento não forem trancáveis, eles deverão estar localizados em uma sala cujo acesso seja restrito ao pessoal autorizado; e

4.7.3. Quando a mídia física estiver em um ambiente (ou sala) no qual não seja possível o seu armazenamento em local com trancas, o próprio ambiente (ou sala) deverá ser trancado quando não estiver em uso (consulte também 4.6.1 acima).

4.8. Retenção e descarte de informações

4.8.1. O /asbz, por meio de suas áreas internas, deve sempre buscar o tratamento de Dados Pessoais estritamente necessários ao atendimento da finalidade pretendida, dispensada a coleta excessiva de dados;

4.8.2. As informações devem ser mantidas apenas pelo tempo necessário para cumprimento de sua finalidade pretendida;

4.8.3. É vedado armazenar fotos, arquivos ou filmes pessoais no disco das máquinas do /asbz, para não ocasionar consumo das unidades de armazenamento com dados não alinhados ao negócio. Caso esses tipos de arquivos sejam encontrados pelo Departamento de Tecnologia da Informação, eles poderão ser apagados sem prévio aviso aos(às) Usuários(as);

4.8.4. Em caso de dúvida sobre o período de armazenamento de determinada informação, os(as) Usuários(as) devem consultar a norma específica que define o tipo de informação que deve ser mantida pelas áreas, juntamente com os períodos de retenção; e

4.8.5. Em caso de qualquer indício de anormalidade ou de suspeita de segurança relativa ao armazenamento dos dados, os(as) Usuários(as) deverão imediatamente comunicar o ocorrido por meio do e-mail do(a) Diretor(a) de Inovação do /asbz e incidentes@asbz.com.br.

4.9. Correio Eletrônico

4.9.1. O /asbz providencia o uso de um sistema de correio eletrônico como ferramenta essencial para que os(as) Usuários(as) o utilizem para fins exclusivamente profissionais;

4.9.2. Nenhum(a) Usuário(a) deve enviar mensagens que possam ser interpretadas como ofensivas, por qualquer outra pessoa, física ou jurídica;

4.9.3. Nenhum(a) Usuário(a) deve transmitir ou retransmitir mensagens que infrinjam o quanto disposto no Código de Conduta e Ética do /asbz.

4.9.4. Não participar de "correntes" de qualquer natureza, malas diretas, abaixo assinados, etc.; e

4.9.5. Os(As) Usuários(as) deverão agir com zelo e atenção em relação à abertura de itens do correio eletrônico, devendo imediatamente comunicar qualquer suspeita de recebimento de spams, *phishing* e similares ao Departamento de Tecnologia da Informação e ao Encarregado pelo Tratamento de Dados do escritório, para que, em conjunto, possam avaliar as medidas necessárias a serem tomadas.

4.10. Internet

4.10.1. O /asbz providencia o acesso à Internet como ferramenta essencial para que os(as) Usuários(as) o utilizem para fins exclusivamente profissionais; e

4.10.2. Nenhum(a) Usuário(a) deve utilizar a Internet de forma a infringir o quanto disposto no Código de Conduta e Ética do /asbz.

4.11. Identificação

4.11.1. Os dispositivos de identificação e senhas protegem a identidade dos Usuários(as), evitando e prevenindo que uma pessoa se faça passar por outra perante o /asbz e/ou terceiros;

4.11.2. Todos os dispositivos de identificação utilizados pelo /asbz, tais como o número de registro dos(as) Usuários(as), o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira;

4.11.3. Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese. O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade);

4.11.4. Os(As) Usuários(as) deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente;

4.11.5. É de responsabilidade de cada Usuário(a) a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados;

4.11.6. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, Bloco de Notas, etc.) compreensíveis por linguagem humana (não criptografados) ou em navegadores. Elas não devem ser baseadas em informações de cunho pessoal, como o próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento e não devem ser constituídas de combinações óbvias de teclado, entre outras;

4.11.7. Após 3 (três) tentativas de acesso a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com o Departamento de Tecnologia da Informação do /asbz, havendo um processo para a renovação de senha;

4.11.8. Senhas provisórias fornecidas pelo Departamento de Tecnologia da Informação deverão ser substituídas por senhas pessoais definitivas de forma imediata;

4.11.9. Os(As) Usuários podem alterar a própria senha, e devem ser orientados a fazêlo, caso suspeitem que terceiros obtiveram acesso indevido as suas credenciais de acesso; e

4.11.10. O período máximo para que seja exigida a troca das senhas é de 90 (noventa) dias, não podendo ser repetidas as 3 (três) últimas senhas. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

4.12. Compartilhamento e divulgação de informações

4.12.1. Quando necessário, o compartilhamento de informações, em especial as que contenham Dados Pessoais e informações confidenciais, seja entre as áreas internas do /asbz ou com terceiros – tais como clientes, transportadoras e prestadores de serviços – deve se dar por meios seguros, disponibilizados e validados pelo /asbz para tal finalidade, devendo ser evitada a utilização de *WhatsApp, Telegram* ou meios similares não dotados de devida segurança;

4.13. Direitos autorais e de terceiros

4.13.1. Não se deve instalar, utilizar ou copiar qualquer peça de software a menos que expressamente permitido pelo legal detentor dos direitos autorais e/ou pelo Departamento de Tecnologia da Informação;

4.13.2. É vedado utilizar dos ativos de informação para armazenar, transmitir ou divulgar livros, músicas, filmes ou quaisquer outros arquivos que estejam protegidos por direito autoral sem a devida permissão do(a) autor(a), ou caso a situação figure dentre as limitações de direitos de autor previstas no art. 46 da Lei de Direitos Autorais; e

4.13.3. Qualquer Usuário(a) que tenha conhecimento da reprodução não autorizada de softwares, livros, vídeos, ou quaisquer outros, dentro do /asbz, deverá notificar imediatamente ao Departamento de Tecnologia da Informação.

4.14. Conduta e Ética

4.12.1 Os(As) Usuários(as) do /asbz devem seguir as diretrizes do Código de Ética e Conduta do /asbz. Também devem atuar de forma responsável nas mídias sociais, em especial as de cunho profissional, das quais façam parte, vedando a publicação de conteúdos com abordagens desrespeitosas, discriminatórias ou que possam gerar um entendimento desfavorável, tanto ao(à) profissional quanto ao /asbz. Os(As) Usuários(as) não devem postar imagens ou comentários que possam revelar Informações Confidenciais do /asbz ou de clientes e não devem emitir juízo de valor sobre o /asbz, parceiros, clientes, concorrentes ou colegas de trabalho.

4.15. Processos de Auditoria

4.15.1. O /asbz se reserva ao direito de executar processos de auditoria interna ou externa a qualquer tempo e sem comunicação prévia aos(às) Usuários(as).

4.16. Partes externas

4.16.1. Os contratos de prestação de serviço celebrados pelo /asbz, em que as contratadas terão acesso às informações, aos sistemas e/ou ao ambiente tecnológico do /asbz devem conter cláusulas que (i) garantam a confidencialidade entre as partes, (ii) disponham sobre a proteção e privacidade dos Dados Pessoais envolvidos, (iii) estabeleçam limites de responsabilidade em caso de uso indevido de tais dados, bem como (iv) assegurem, minimamente, que os(as) profissionais sob sua responsabilidade cumpram a presente Política e as demais normas de Segurança da Informação do /asbz, seguindo as diretrizes do Código de Ética e Conduta do /asbz.

5. Casos Omissos

5.1. Os casos omissos serão avaliados pelo Grupo de Trabalho de Segurança da Informação para posterior deliberação;

5.2. As diretrizes estabelecidas nesta Política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do(a) Usuário(a) da informação do /asbz adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção as informações do /asbz; e

5.3. Os casos omissos também devem ser reportados formalmente ao e-mail do(a) Diretor(a) de Inovação do /asbz e incidentes@asbz.com.br.

6. Revisões

6.1.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Grupo de Trabalho de Segurança da Informação.

Data	Versão	Aprovado por
01.04.2022	1	Comitê de Gestão Institucional e Diretoria Executiva

(* * *)