POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA BOWE

Versão 1.0/2024

FOLHA DE CONTROLE

Título	Política de Segurança da Informação
Número da versão	V01/2024
Status	Elaboração do Documento
Órgão Aprovador	Diretoria
Data da Aprovação	05/01/2024
Área responsável pela elaboração	Jurídico Externo - NDM Advogados e Setor de Segurança da Informação
Área de aplicação	Brasil
Classificação da Publicidade	Público interno

1. INTRODUÇÃO

A Política de Segurança da Informação ("Política") tem como objetivo estabelecer as regras, procedimentos e controles de Segurança da Informação da **BOWE LTDA.** ("**BOWE**"), conforme as previsões regulatórias.

A Segurança da Informação pode ser entendida como a capacidade de prevenir, detectar, responder e de se recuperar rapidamente de uma ameaça cibernética, a fim de proteger a confidencialidade, integridade e disponibilidade dos ativos tecnológicos e informações.

Dessa forma, o objetivo desta política é descrever o uso aceitável de equipamentos de informática da **BOWE**. Essas regras estão em vigor para proteger nossos parceiros, colaboradores e a própria empresa do uso inapropriado desses ativos que possam expor a **BOWE** a riscos, incluindo ataques de vírus, comprometimento de sistemas e serviços de rede, situações reputacionais e violações legais.

Por meio desta Política buscamos manter os Princípios do Privacy by Design, mantendo a funcionalidade total das operações. Isso quer dizer que o documento não tem o objetivo de impor restrições que sejam contrárias à cultura estabelecida na **BOWE** de abertura, confiança e integridade e sim ter uma abordagem "risk oriented", contra ações ilegais ou prejudiciais por parte de indivíduos, conscientes ou não.

Ainda, esta Política visa viabilizar a identificação de possíveis violações de Segurança da Informação por meio da definição de ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e digitais, a fim de mitigar, assim, os riscos de segurança da informação, garantindo, ainda, a continuidade de seus negócios, protegendo os processos críticos de interrupções causadas por falhas ou desastres.

Ressalta-se que esta Política é condizente com:

I – o porte, o perfil de risco e o modelo de negócio da **BOWE**.

II – a natureza das suas atividades e a complexidade dos serviços e produtos por ela fornecidos.

III – a sensibilidade dos dados e das informações sob responsabilidade da **BOWE**.

2. NORMAS DE REFERÊNCIA

Normas que servem de referência para a elaboração desta Política:

- Lei Geral de Proteção de Dados (Lei n.º 13.709/2018);
- Resolução CD/ANPD n.º 2 de janeiro de 2022.

3. ÂMBITO DE APLICAÇÃO

A Presente Política será aplicável a todos os Colaboradores, membros da Alta Administração, Terceiros e quaisquer outras pessoas, sejam físicas ou jurídicas, que tenham ou venham a ter acesso aos dados controlados e ao sistema de informação da **BOWE**.

3.1. O não cumprimento desta Política

O não cumprimento desta Política acarretará sanções administrativas, podendo acarretar o desligamento do colaborador ou rescisão do contrato vigente e a reparação de danos, de acordo com a gravidade da ocorrência.

4. DEFINIÇÕES

Visando auxiliar na interpretação e aplicação desta Política, as palavras com iniciais maiúsculas, seja no singular ou no plural, devem ser entendidas da seguinte forma:

- Alta Administração se refere aos membros que compõem a diretoria executiva e o conselho da administração, caso esteja implementado.
- Colaborador(es) se refere aos empregados contratados sob o regime da CLT, estagiários e jovens aprendizes.
- Terceiro(s) se refere aos prestadores de serviços, parceiros comerciais, dentre outras pessoas jurídicas ou físicas que se relacionem comercialmente com a **BOWE**.
- Cliente(s) se refere aos usuários que adquirem ou utilizem de alguma forma os serviços da **BOWE**.
- Controlador(es) se refere às empresas que contratam o sistema **BOWE.**
- ANPD se refere à Autoridade Nacional de Proteção de Dados.
- Incidente de segurança com dados pessoais: Conforme definição da ANPD:

  > Incidente de segurança com dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

5. GOVERNANÇA

A Governança em Proteção de Dados e Segurança da Informação será definida pela Política de Governança em Proteção de Dados.

6. DIRETRIZES GERAIS DE RESPONSABILIDADE E CONFORMIDADE

Esta Política tem o intuito de assegurar a proteção dos ativos de informação contra ameaças, internas ou externas, reduzir a exposição a perdas ou danos decorrentes de falhas de segurança da informação e garantir que os recursos adequados estarão disponíveis, mantendo um programa de segurança efetivo e conscientizando Colaboradores e Terceiros acerca do tema.

Os processos de segurança de dados e da informação da **BOWE** devem assegurar a:

- Confidencialidade: Garantia de que a informação somente estará acessível para pessoas autorizadas.
- Integridade: Garantia de que a informação, armazenada ou em trânsito, não sofrerá qualquer modificação não autorizada, seja esta intencional ou não.
- Disponibilidade: Garantia de que a informação estará disponível sempre que for necessário.
- Autenticidade: Garantia sobre a fonte segura da informação.
- Não repúdio: Garantia de monitoramento de uso, evitando negativa de autoria.

Ainda, a **BOWE** assegura que:

- Todos os dados pessoais coletados serão tratados conforme a Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709 de 2018), sendo utilizados somente para a finalidade para a qual foram coletados;
- Baseará a gestão de seus sistemas e ambientes virtuais com base em análises de riscos revisadas periodicamente;
- A definição e implementação de controles terá como parâmetro normas nacionais e internacionalmente reconhecidas na área de sistemas de gestão de segurança da informação e segurança da informação;
- Com base nas avaliações de riscos e perfil da organização será elaborado cenário de incidentes considerados nos testes de continuidade dos serviços;
- Classifica os dados e as informações quanto à relevância;
- Divulga e capacita a sua equipe, a fim de disseminar a cultura de segurança da informação.

6.1. Diretrizes Gerais de Responsabilização e Conformidade

Ainda, a **BOWE** poderá realizar auditorias e monitoramento em suas redes, dispositivos e sistemas periodicamente para garantir a conformidade com esta Política.

6.1.1. Novos Dispositivos: Para que novos dispositivos sejam incluídos na rede e ao sistema, a aprovação explícita pelo gestor competente é necessária.

6.1.2. Autenticação: Todo uso de tecnologia ou dispositivos deve ser autenticado com ID de usuário e senha ou outro item de autenticação (por exemplo, token), conforme Política de Senha Segura.

6.1.3. Rastreamento: Todas as tecnologias ou dispositivos exigem uma lista de todo o pessoal autorizado a usar os dispositivos, conforme princípios de need to know.

6.1.4. Marcação: Todas as tecnologias ou dispositivos exigem rotulagem de dispositivos com proprietário, informações de contato e finalidade.

6.1.5. Classificação e Acesso à Informação: As informações devem ser classificadas e acessadas de acordo com estas Políticas.

6.1.6. Laptops: Como as informações contidas em Notebooks são especialmente vulneráveis, deve-se ter cuidado especial. Dessa forma o uso dos mesmos deve ser realizado conforme o presente documento.

6.1.7. Software antivírus: O uso de software de proteção contra vírus deve estar em conformidade com o presente instrumento.

6.1.8. E-mail: A comunicação via e-mail e utilização dessas ferramentas deve estar em conformidade com o presente instrumento.

6.1.9. Usos Proibidos: Os ativos, sistemas e bens da **BOWE** em nenhuma circunstância poderão ser utilizados para atividades ilícitas ou que vão de encontro com os objetivos, missão e cultura da empresa, assim como suas Políticas internas. A lista, a seguir, de condutas proibidas é exemplificativa. São terminantemente proibidos(as):

6.1.9.1. A distribuição ou acesso de Informações Confidenciais, restritas por pessoas que não possuam a devida autorização de segurança.

6.1.9.2. Violações dos direitos de qualquer pessoa ou empresa protegida por direitos autorais, segredo comercial, patente ou outra propriedade intelectual, ou leis ou regulamentos semelhantes, incluindo, mas não limitado à instalação ou distribuição de produtos de software "pirateados" ou outros que não sejam devidamente licenciados para uso pela **BOWE**.

6.1.9.3. Realização ou uso de cópia não autorizada de material protegido por direitos autorais, incluindo, mas não limitado a digitalização e distribuição de fotografias de revistas, livros ou outras fontes protegidas por direitos autorais, música protegida por direitos autorais e a instalação de qualquer software protegido por direitos autorais para o qual a **BOWE** ou o usuário final não tenha uma licença ativa.

6.1.9.4. A exportação de software, informações técnicas, software ou tecnologia de criptografia, em violação às leis

internacionais ou regionais de controle de exportação, sem a devida autorização.

6.1.9.5. A introdução de programas maliciosos na rede ou servidor da **BOWE** ou de Terceiros (por exemplo, vírus, worms, cavalos de tróia, bombas de e-mail, etc.).

6.1.9.6. A revelação da senha de contas de acesso para outras pessoas ou permissão do uso de contas de acesso por outras pessoas. Isso inclui familiares e outros membros da família quando o trabalho está sendo feito em casa.

6.1.9.7. O uso de um ativo de computação da **BOWE** para se envolver ativamente na aquisição ou transmissão de material que viole as leis de assédio sexual ou locais de trabalho hostis na jurisdição local do usuário.

6.1.9.8. A feitura de ofertas fraudulentas de produtos, itens ou serviços provenientes de qualquer conta da **BOWE**.

6.1.9.9. Efetuar violações de segurança ou interrupções de comunicação de rede. As violações de segurança incluem, mas não se limitam, a acessar dados dos quais o funcionário não é um destinatário pretendido ou fazer login em um servidor ou conta que o funcionário não está expressamente autorizado a acessar, a menos que essas funções estejam dentro do escopo das funções normais. Para os propósitos desta seção, "interrupção" inclui, mas não se limita a, detecção de rede, inundações de ping, falsificação de pacotes, negação de serviço e informações de roteamento forjadas para fins maliciosos.

6.1.9.10. A varredura de portas ou varredura de segurança de forma independente é expressamente proibida, a menos que seja feita uma notificação prévia ao Gestor Responsável.

6.1.9.11. Executar qualquer forma de monitoramento de rede que intercepte dados, a menos que essa atividade faça parte do trabalho/dever normal do funcionário.

6.1.9.12. Contornar a autenticação do usuário ou a segurança de qualquer host, rede ou conta.

6.1.9.13. Usar qualquer programa/script/comando ou enviar mensagens de qualquer tipo com a intenção de interferir ou desabilitar a sessão do terminal de um usuário, por qualquer meio, localmente ou via Internet/Intranet/Extranet.

6.1.9.14. Revelar informações ou listas de funcionários da **BOWE** para terceiros.

6.1.9.15. Realizar o envio de mensagens de e-mail não solicitadas, incluindo o envio de "lixo eletrônico" ou outro material publicitário para indivíduos que não solicitaram especificamente esse material (spam de e-mail).

6.1.9.16. Envio de PANs (números de cartão de crédito) não criptografados por qualquer tecnologia de mensagens do usuário final (e-mail, mensagens instantâneas, bate-papo).
6.1.9.17. Realizar qualquer forma de assédio via qualquer canal de comunicação.
6.1.9.18. Realizar o uso não autorizado ou falsificação de informações de cabeçalho de e-mail.
6.1.9.19. Criação ou encaminhamento de "correntes", "Ponzi" ou outros esquemas de "pirâmide" de qualquer tipo.
6.1.9.20. Publicar mensagens não relacionadas a negócios iguais ou semelhantes em muitos grupos de notícias Usenet (spam de grupo de notícias).

6.1.10. *Wireless*: A **BOWE**, quando possível, oferece aos seus contratados, funcionários, colaboradores e parceiros, uma rede sem fio (Wi-Fi) própria, para finalidades estritamente profissionais. Para ter acesso ao Wi-Fi a pessoa deverá ser expressamente autorizada pela **BOWE** e deverá se comprometer a fazer o uso seguro desse recurso. Excepcionalmente, visitantes, fornecedores e afins poderão ter acesso à rede sem fio, devendo obter autorização expressa da **BOWE**.

7. PROCEDIMENTOS E CONTROLES

7.1. Políticas de Classificação de Dados

As informações, dados e documentos operados pela **BOWE** serão classificados de acordo com as categorias abaixo indicadas, considerando a sensibilidade e a relevância do seu conteúdo para a **BOWE** e para os seus Clientes:

- Nível 01 - Documentos Públicos: Informações aprovadas pela Alta Administração para uso público (interno e externo), por exemplo relatórios anuais, indicações para a imprensa, etc.;
- Nível 02 - Somente Uso Interno: Informação não aprovada para circulação fora da **BOWE** como, por exemplo memorandos internos, minutas e/ou atas de reuniões, procedimentos, rotinas operacionais e relatórios de projetos internos;
- Nível 03 - Confidencial: Informações cuja circulação interna é controlada por questões estratégicas e de gestão, e cuja circulação externa é vedada, pois se tornadas públicas ou compartilhadas causarão impacto e prejuízos aos negócios, podendo ser planos estratégicos e especificações que definem a forma que a organização opera, informações contábeis, planos de negócio, informações sobre clientes ou acionistas, dentre outros. Este nível envolve todas as Informações e Dados referentes aos Clientes da **BOWE**, inclusive dados pessoais.

- Nível 04 - Informações Sensíveis: Informações internas ou confidenciais críticas ao desenvolvimento das atividades da **BOWE**, que (i) são referentes a dados pessoais sensíveis e de crianças e adolescentes (ii) são acobertadas por sigilo bancário, nos termos da legislação aplicável; e/ou (ii) cuja perda ou indisponibilidade pode prejudicar ou impedir a adequada prestação de serviços pela **BOWE** aos clientes, a realização de operações da **BOWE** e/ou o cumprimento de suas obrigações legais e/ou normativas.

7.1.1. Políticas de Restrição de Acessos

Apenas poderão ter acesso a informações aqueles indivíduos que realmente precisam saber sobre elas para desempenhar suas atividades. O acesso às informações se dará conforme os seguintes requisitos:

- Nível 01: Livre acesso.
- Nível 02: Funcionários e não funcionários da **BOWE** com acordos de confidencialidade assinados que têm uma necessidade comercial de saber.
- Nível 03: Somente os indivíduos designados com acesso aprovado e acordos de confidencialidade assinados.
- Nível 04: Somente os indivíduos designados com acesso aprovado e acordos de confidencialidade assinados. O acesso deve ser restrito a poucos colaboradores, de preferência gestores.

7.2. Políticas de Sistemas Antivírus

Com o objetivo de prevenir acessos indevidos e incidentes de informação é necessário que todos os ativos aplicáveis sejam utilizados apenas caso os sistemas Antivírus estejam corretamente instalados e programados para serem executados em intervalos regulares (diariamente). São as regras:

- O software antivírus e os arquivos de padrão de vírus devem ser mantidos atualizados.
- O software antivírus deve manter logs de atividade por um período mínimo de 1 (um) ano.
- Os computadores infectados por vírus devem ser removidos da rede até que sejam verificados como livres de vírus.
- Os administradores de sistema e de rede são responsáveis por criar procedimentos que garantam que o software antivírus seja executado em intervalos regulares e que os computadores sejam verificados como livres de vírus.
- Quaisquer atividades com a intenção de criar e/ou distribuir programas maliciosos nas redes da **BOWE** (por exemplo vírus, worms, cavalos de tróia, bombas de e-mail, etc) são proibidas.
- Todos os dispositivos móveis e de propriedade dos sujeitos a esta Política que se conectam à rede da **BOWE** ou a Internet mesmo quando

estão fora da rede exigem que um software de firewall pessoal seja instalado, configurado corretamente e executado ativamente.

- O administrador do sistema é responsável por configurar o software de firewall pessoal para não ser alterado por usuários de dispositivos móveis ou de propriedade de funcionários.

7.3. Políticas de Auditoria

A **BOWE** se reserva no direito de auditar qualquer dispositivo utilizado pelos indivíduos sujeitos a esta Política durante o desempenho das atividades comerciais ou funções. Para este fim serão solicitados os acessos, que podem incluir (rol exemplificativo):

- Nível de usuário e/ou acesso em nível de sistema a qualquer computação ou comunicação;
- Acesso às informações (eletrônicas, impressas, etc.) que possam ser produzidas, transmitidas ou armazenadas em equipamentos ou instalações da **BOWE**;
- Acesso às áreas de trabalho (escritórios, cubículos, áreas de armazenamento, data centers, centros de operações, etc.);
- Acesso para monitorar e registrar interativamente o tráfego nas redes da **BOWE**.

Esta auditoria deve observar as regras da Lei Geral de Proteção de Dados e sua possibilidade informada na Comunicação Interna de Privacidade aos colaboradores da **BOWE**.

7.4. Políticas de Dispositivos Desktop e Laptop

Com o objetivo de manter a segurança em dispositivos locais, será necessário a adoção das seguintes medidas:

- Os usuários de desktops e laptops devem concordar em assumir responsabilidade compartilhada pela segurança de seu sistema e pelas informações nele contidas.
- Ao alocar um desktop ou laptop, o usuário deve preencher um Formulário de Usuário de Desktop/Laptop e se comprometer a cumprir todas as seções aplicáveis desta Política de Segurança de Desktop e Laptop.
- Desktops e laptops são entregues aos colaboradores da **BOWE**. Quando isso acontece, o usuário assume a "tutela" temporária do sistema.
- Ao deixar a posição na **BOWE**, o indivíduo deve devolver o dispositivo ao seu gerente ou supervisor, assinando novamente seu Formulário de Usuário de Desktop/Laptop original. Isso libera o indivíduo de responsabilidade sobre ações futuras realizadas com este dispositivo.

- Os usuários devem tomar todas as medidas razoáveis para se proteger contra a instalação de software não licenciado ou malicioso, conforme estas Políticas.
- Não é permitido o uso de software não licenciado (pirataria de software).
- Os softwares instalados devem ser validados e aprovados pelo Gestor Responsável. Instalações não gerenciadas podem comprometer o ambiente operacional de TI e também constituir um risco de segurança, incluindo a disseminação intencional ou não intencional de vírus de software e outros softwares mal-intencionados.
- O software comercial (incluindo shareware) deve: a) Ter uma licença válida para cada usuário em potencial; b) Ser verificado quanto a todos os riscos de segurança conhecidos, incluindo software malicioso.
- O Usuário deve proteger seu acesso por senha e não permitir acessos de convidados.
- O Usuário deve proteger o acesso ao seu PC com a tela de bloqueio automático para forçar o usuário a fazer login novamente após 15 (quinze) minutos de inatividade.
- O Usuário deve permitir a execução diária do antivírus, programada pelo Setor Responsável.
- O Usuário deve permitir a atualização regular de seu sistema operacional e aplicativos, como seu navegador, cliente de e-mail, aplicativos de escritório, etc.
- O Usuário não pode instalar ou abrir arquivos recebidos de entidades desconhecidas.
- O Usuário deve desativar os recursos de 'autorun' que acionam qualquer mídia para ser montada e executada assim que for conectada ao PC.
- Os Usuários não devem abrir arquivos executáveis recebidos por e-mail ou pelo navegador (por exemplo, componentes ActiveX).
- O Usuário deve notificar qualquer risco de infecção ao Gestor Responsável.

Adicionalmente, como medidas de segurança, os usuários de laptops devem cumprir as seguintes regras:

- Os laptops não devem ser deixados à vista em um veículo sem vigilância, mesmo por um curto período de tempo.
- Os laptops não devem ser deixados em um veículo durante a noite.
- Os laptops não devem ser posicionados de forma que sejam visíveis do lado de fora de uma janela do andar térreo, a menos que não haja alternativa.
- Um laptop exibindo informações confidenciais sendo usado em um local público, por exemplo, em um avião ou carro, deve, sempre que possível, ser posicionado de forma que sua tela não possa ser vista por

outras pessoas. Se necessário, alguns dispositivos possuem funções para proteger a visão de terceiros posicionados ao lado da tela.

- Em situações vulneráveis, como por exemplo áreas públicas como saguões de aeroportos, hotéis e centros de conferências, o laptop nunca deve ser deixado sem vigilância.
- Os computadores portáteis devem, sempre que permitidos, serem transportados como bagagem de mão ao viajar, de preferência em malas com cores vivas ou etiquetas grandes, pois isso impedirá muitos ladrões em potencial.
- Quando qualquer uma das regras acima for inadequada ou impraticável, o proprietário é responsável por tomar todas as medidas razoáveis para minimizar o risco de perda ou dano do laptop.
- Os usuários de laptop devem empregar o padrão corporativo para criptografia de dados em arquivos e pastas em laptops, por exemplo, Microsoft EFS (Sistema de Arquivos Criptografados) ou PGPDisk.
- Os usuários de laptops devem notificar as autoridades competentes imediatamente se seu laptop for perdido ou roubado.

7.5. Políticas de Email

Para prevenir incidentes de segurança causados por ações dolosas ou culposas no momento da utilização das ferramentas de e-mail, a **BOWE**, adotou as seguintes regras:

É responsabilidade do Usuário a extrema cautela no momento do envio de e-mails em nome da **BOWE** ou em função de suas atividades, evitando, por exemplo, sempre que possível, enviar e-mails para vários destinatários ou com cópia para vários endereços de e-mail e verificando as informações contidas no texto e destinatário antes de enviar.

Todos os e-mails enviados para fontes externas conterão uma isenção de responsabilidade padrão:

> *AVISO: Esta mensagem, incluindo todos os anexos transmitidos com ela, é para uso exclusivo do destinatário e pode conter informações proprietárias, confidenciais e/ou legalmente privilegiadas pertencentes a **BOWE**. Se você não for o destinatário pretendido, não deverá, direta ou indiretamente, usar, divulgar, distribuir, imprimir ou copiar qualquer parte desta mensagem. Se você acredita que recebeu esta mensagem por engano, exclua-a e todas as cópias dela do seu sistema e notifique o remetente imediatamente por e-mail de resposta.*

Os colaboradores devem ter o máximo cuidado ao abrir qualquer e-mail de fonte externa. Embora o e-mail de entrada seja protegido por um sistema antivírus, novos vírus aparecem com muita frequência.

A menos que seja aprovado por seu Gestor, um e-mail interno da **BOWE** não deverá ser encaminhado automaticamente para um destino externo. Informações confidenciais ou restritas, conforme definido na Política de Acesso e Classificação de Informações, não serão encaminhadas por qualquer meio, a menos que esse e-mail seja crítico para os negócios e esteja criptografado.

Os responsáveis pela Segurança da **BOWE** poderão monitorar todos os e-mails de entrada, saída e internos.

Ainda, conforme as sugestões da ANPD, a **BOWE** e seus colaboradores, deverão adotar as seguintes medidas para proteção dos dispositivos móveis da empresa:

- Utilizar, sempre que possível, técnicas de autenticação multi-fator para controle de acesso de dispositivos móveis – como smartphones e laptops, o que inclui aplicações importantes para a operação.
- Separar os dispositivos móveis de uso privado daqueles de uso institucional.
- Implementar funcionalidades que permitam apagar remotamente os dados pessoais armazenados em dispositivos móveis.

7.6. Políticas de Criptografia

Essas medidas têm o objetivo de impor limites e estabelecer requisitos para o uso da criptografia pela **BOWE**. São as regras:

- Algoritmos padrão comprovados, como o AES, devem ser usados como base para tecnologias de criptografia. Esses algoritmos representam a cifra real usada para um aplicativo aprovado. Por exemplo, o Pretty Good Privacy (PGP) da Network Associate usa uma combinação de IDEA, CAST ou 3DES, enquanto o Secure Socket Layer (SSL) usa criptografia RSA.
- Os comprimentos de chave do sistema criptográfico simétrico devem ser de pelo menos 128 bits.
- As chaves do sistema de criptografia assimétricas devem ter um comprimento que produza força equivalente.
- Os requisitos de comprimento de chave da **BOWE** serão revisados anualmente e atualizados conforme a tecnologia permitir.
- O uso de 'proprietary encryption algorithms' não é permitido para qualquer finalidade, a menos que seja revisado por especialistas qualificados fora do fornecedor em questão e aprovado pela **BOWE**.

7.7. Prevenção à Incidente de Segurança ocasionado por Colaboradores ou Terceiros

7.7.1. Concessão de Acesso aos Sistemas e Monitoramento

A Diretoria exigirá a assinatura de Termo de Confidencialidade e Sigilo com os Colaboradores e Terceiros envolvidos nas operações da **BOWE**, bem como indicará quem são os gestores responsáveis por conceder, limitar, excluir e suprimir o acesso aos sistemas e ambientes virtuais da **BOWE**, de forma que a **BOWE** contará com mecanismos de cadastro, autenticação e de rastreio das ações (logs dos históricos) realizadas por seus Colaboradores e Terceiros, que, porventura, tenha acesso aos seus sistemas.

Os ambientes de trabalho que guardem computadores, servidores, dentre outros dispositivos eletrônicos que permitam acesso aos sistemas e ambientes virtuais da **BOWE**, serão monitorados por câmeras 24h (vinte e quatro horas) por dia, 7 (sete) dias da semana.

Ademais, os Colaboradores que em decorrência da sua função precisam ter acesso a dados pessoais de Clientes e informações delicadas quanto à sua saúde financeira, utilização dos produtos da **BOWE**, dentre outros dados, serão de preferência alocados em locais específicos dentro da empresa, a fim de reduzir as chances de comunicação de informações confidenciais para Colaboradores que não necessitem de tal informação.

A **BOWE** manterá **canal de denúncia anônimo** disponível aos Colaboradores para que possam relatar condutas suspeitas de colegas ou de Terceiros, bem como realizará periodicamente auditorias internas, com o objetivo de avaliar o histórico de acessos (logs) de Colaboradores, a fim de diagnosticar eventual conduta suspeita ou irregular, bem como irá requerer o mesmo padrão de zelo e de gestão das empresas de processamento, armazenamento e computação em nuvem contratadas.

7.7.2. Uso de equipamentos corporativos, responsabilidade com os dados de acesso e restrições de acesso

A **BOWE** fornecerá os equipamentos eletrônicos que sejam necessários a execução das atividades pelo Colaborador, tais como: laptops, pen-drives, tablets, celulares, dentre outros, podendo assim realizar varreduras e investigações internas nos

equipamentos corporativos. Além disso, a **BOWE** se propõe a implementar em seus equipamentos e sistemas um sistema de controle de acesso aplicável a todos os usuários, com níveis de permissão na proporção da necessidade de trabalhar com o sistema e de acessar dados pessoais, conforme determinado nestas Políticas.

Os Colaboradores são responsáveis por todos os atos executados com seu identificador (login), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia, estando proibido de ceder ou facilitar o uso do seu identificador ou o uso de equipamentos por outras pessoas,. Ainda, enquanto estiver ausente deverá bloqueá-los. Outros detalhes constam no decorrer da presente Política.

7.8. Prevenção à Indisponibilidade do Sistema e Ambientes Virtuais da BOWE

A **BOWE** dedica equipe interna específica para a implementação de melhorias e monitoramento da integridade do sistema e ambientes virtuais. Ademais, para reduzir as chances de indisponibilidade tem como medidas de controle:

- Redundância de links de internet e de servidores;
- Load balance;
- Assistência externa com o provedor de internet com SLA máximo de 4h (quatro horas) para a solução, quando estiver sem acesso à rede.

7.8.1. Manutenção e Cópias de Segurança

A **BOWE** realiza cópias de Segurança (Backup) e recuperação (Restore) de dados e informações, inclusive das informações e dados que, porventura, estejam sendo processados e armazenados por prestadores de serviços localizados no Brasil ou no exterior, adotando medidas administrativas que visem a sua integridade e inviolabilidade.

7.8.2. Informações e Proteção aos Clientes

A **BOWE** disponibiliza em seu sistema os Termos de Uso e Aviso de Privacidade, pelos quais será possível verificar as condições gerais dos serviços disponíveis e de utilização da plataforma, além de informar as empresas terceiras que terão acesso aos dados pessoais, para fins de prestação dos serviços.

7.9. Segurança das Comunicações

Para garantir a segurança das Comunicações a **BOWE** deve sempre:

- Utilizar conexões cifradas (TLS/HTTPS) ou aplicativos com criptografia fim- a fim para serviços de comunicação.
- Instalar e manter um sistema de firewall e/ou utilizar um Web Application Firewall (WAF – Filtro de Aplicação).
- Proteger e-mails via adoção de ferramentas AntiSpam, filtros de e-mail e integrar o antivírus ao sistema de e-mail.
- Remover quaisquer dados sensíveis e outros dados pessoais que estejam desnecessariamente disponibilizados em redes públicas.

7.10. Da contratação de serviços de processamento, armazenamento de dados e de computação em nuvem

A **BOWE** realiza avaliações prévias (Due Diligence) para efetivar a contratação de terceiros prestadores de serviços de processamento, armazenamento de dados e de computação em nuvem, seja no Brasil ou no exterior, de forma que as práticas de verificação a serem adotadas consideram a: i. criticidade do serviço e ii. sensibilidade dos dados e informações a serem processados, armazenados e gerenciados, levando em conta ainda a classificação prevista no item 6.1 desta Política.

A **BOWE** poderá adotar as seguintes práticas:

- Necessidade de ter obtido e estar válida certificação de segurança da informação, tais como: PCI DSS e ISO 270001, dentre outras certificações aplicáveis.
- Pesquisa prévia utilizando banco de dados público ou privado.
- Solicitação de preenchimento de formulário e envio de documentos e informações.
- Visitas técnicas.
- Auditoria realizada por empresa externa independente especializada.
- Solicitação de contratação de seguro contra vazamento de dados.
- Previsão contratual de responsabilidade por incidente de dados pessoais ocasionados por sua culpa ou dolo.
- Realizar contrato de acordo de nível de serviço com o provedor de serviços em nuvem, contemplando a segurança dos dados armazenados.
- Avaliar se o serviço oferecido pelo provedor do serviço em nuvem atende os demais requisitos de segurança da informação estabelecidos.
- Analisar os requisitos para o acesso do usuário a cada serviço em nuvem utilizado.
- Utilizar técnicas de autenticação multi-fator para acesso aos serviços em nuvem relacionados a dados pessoais.
- O Contratado deverá cumprir com o Guia da ANPD de Segurança da Informação.

- Ainda, no momento de extinção contratual o prestador de serviços deverá:
    - Transferir os dados ao novo prestador ou à **BOWE**.
    - Confirmar a integridade e disponibilidade dos dados transferidos e, após isso, excluí-los de sua base.

7.11. Políticas de Senha Segura

As senhas utilizadas em nível profissional em atividades ligadas a **BOWE** devem respeitar as seguintes regras:

- Os usuários nunca devem compartilhar sua senha com outros usuários.
- Todas as senhas de nível de sistema (por exemplo: root, enable, NT admin, contas de administração de aplicativos, etc.) devem ser alteradas pelo menos a cada 90 (noventa) dias.
- Todas as senhas de nível de sistema de produção devem fazer parte do banco de dados global.
- Todas as senhas de nível de usuário (por exemplo, e-mail, web, computador desktop, desenvolvimento, sistema de contabilidade do comerciante, produção, etc.) devem ser alteradas pelo menos a cada 90 (noventa) dias.
- As contas de usuário que têm privilégios de nível de sistema concedidos por meio de associações a grupos ou programas devem ter uma senha exclusiva e diferente de todas as outras contas mantidas por esse usuário.
- As senhas não devem ser inseridas em mensagens de e-mail ou outras formas de comunicação eletrônica.
- A reutilização de senhas em diferentes níveis de administração e uso do sistema não é permitida.
- Trimestralmente, um software de quebra de senha será usado para identificar aleatoriamente senhas fracas e pedir aos proprietários das contas que as alterem imediatamente.
- Todas as senhas de backoffice inativas devem ser revogadas após 90 (noventa) dias.
- O acesso ao servidor de banco de dados é conhecido apenas pelo Administrador
- Os Usuários não devem imprimir ou escrever em papel suas senhas. O ideal é que memorizem e não mantenham nenhum rastro. No entanto, é possível usar alguma ajuda de memória com truques para lembrá-lo.
- O Usuário deve usar sempre senhas de, no mínimo, 8 (oito) caracteres, misturando letras e dígitos. Ainda, não deve usar informações pessoais ou palavras de dicionário para gerar sua senha.
- O Usuário deve observar que será obrigado a escolher uma nova senha para o backoffice de gerenciamento pelo menos uma vez a cada

90 (noventa) dias e não poderá usar uma das últimas quatro senhas que tinha antes.

- Se desenvolvedores, funcionários ou clientes tiverem acesso aos ambientes de produção e teste, as credenciais usadas para acessar um ou outro devem ser diferentes.

7.12. Políticas de Análises de Riscos

A execução, desenvolvimento e implementação de programas de análises de riscos são de responsabilidade da área de segurança da informação. Espera-se que os funcionários cooperem totalmente com qualquer análise conduzida em sistemas pelos quais são responsáveis. Espera-se também que os funcionários trabalhem conjuntamente no desenvolvimento de um plano de gestão de risco e remediação. Avaliações preliminares de risco serão sempre realizadas quando ocorrerem:

- Grandes Pedidos de Alteração.
- Grandes mudanças nos sistemas e redes responsáveis pelo transporte ou processamento de informações confidenciais ou restritas, incluindo novos equipamentos de rede, novos sistemas operacionais e novos servidores de correio.
- Novas interfaces para processadores de terceiros ou integradores de sistemas.

7.12.1. Processo de Avaliação de Risco

As análises de risco devem conter, ao menos, os seguintes componentes:

- Atribuir um nível de risco;
- Atribuir valores para probabilidade e impacto do evento negativo, conforme matriz previamente aprovada;
- Determinar qual nível de segurança existe no momento;
- Verificar possibilidade de Risco inerente;
- Estabelecer medidas complementares e realizar a gestão do risco.

O risco é definido como uma função da probabilidade de um evento negativo se concretizar e da magnitude da perda se ocorrer. Os seguintes níveis de risco são usados no processo de avaliação:

- Risco mínimo;
- Baixo risco;
- Risco moderado;
- Alto risco;
- Risco máximo.

7.13. Política de Desenvolvimento Seguro de Software

Caso vá realizar o desenvolvimento próprio, mesmo que por mão de obra de terceiros, de sistemas e softwares, a **BOWE** deverá estabelecer uma Política de Desenvolvimento Seguro de Software.

8. POLÍTICAS DE RETENÇÃO DE DADOS

A **BOWE** deverá manterPolítica de Retenção de Dados, levando em consideração as normas aplicáveis, principalmente relacionadas aos dados pessoais.

9. PLANO DE RESPOSTAS A INCIDENTES

A **BOWE** deve elaborar cenários de incidentes, no âmbito dos testes de continuidade dos negócios, visando mapear os eventos capazes de dificultar a operação dos agentes computacionais ou humanos que provocam queda no desempenho, obstrução ou erro na execução de um ou mais processos organizacionais e impossibilitam a plena operação dos serviços. Além disso, deverá manter a Política de Resposta a Incidentes de Segurança aplicada e difundida na empresa.

Ainda, em caso de incidentes, como interceptações, compartilhamentos ou vazamentos de informações, o Colaborador ou Terceiro tem o dever de informar o Departamento de Tecnologia da **BOWE** ou o seu Encarregado de Dados, em um prazo máximo de 2 (duas) horas para que todas as medidas de segurança sejam tomadas.

10. CAPACITAÇÃO DE COLABORADORES E TERCEIROS

A equipe da **BOWE** manterá comunicação ativa e periódica sobre os termos desta Política, de modo que os Colaboradores e Terceiros que prestem serviços relevantes e relacionados com ela passarão por capacitações, com o objetivo de esclarecer a interpretação e aplicação desta Política, bem como informá-los sobre temas atrelados a ela, tais como: proteção de dados pessoais, segurança da informação, políticas de consequências, dentre outros.

Além disso, a equipe **BOWE** será responsável por orientar os Colaboradores para não desativarem ou ignorarem as configurações de segurança de estações de trabalho, realizar backups offline, periódicos e armazená-los de forma segura, além de inventariar e cifrar dados de dispositivos externos. Os treinamentos devem conter no mínimo:

- Como utilizar controles de segurança dos sistemas de TI relacionados ao trabalho diário;
- Como evitar de se tornarem vítimas de incidentes de segurança corriqueiros, tais como contaminação por vírus ou ataques de phishing, que podem ocorrer, por exemplo, ao clicar em links recebidos na forma de pop-up de ofertas promocionais ou em links desconhecidos que chegam por e-mail;

- Manter documentos físicos que contenham dados pessoais dentro de gavetas e não sobre as mesas;
- Não compartilhar logins e senhas de acesso das estações de trabalho;
- Bloquear os computadores quando se afastar das estações de trabalho, para evitar o acesso indevido de terceiros;
- Seguir as orientações da Política de Segurança da Informação.

11. VIGÊNCIA

A presente Política foi aprovada pela Diretoria Executiva, de forma que o presente documento entra em vigor em 05/01/2024 e será revisado no período máximo de 01 (um) ano ou havendo necessidade anterior, o que for menor, para que o documento permaneça sempre atualizado.

Em caso de dúvidas acerca desta Política, por favor, entre em contato com Bianca, através do e-mail juridico@smartech.digital.