CONTROLE DE REVISÃO DE DOCUMENTOS		
REV	DATA	DESCRIÇÃO
0	01/07/2023	EMISSÃO INICIAL

ÍNDICE

1. INTRODUÇÃO

A BOSLTER CONSULTANCY - BC é uma empresa com fins econômicos, que atua há mais de 8 anos, empresa mineira especializada em soluções de treinamentos, consultorias e guarda e gestão de documentos. Desde 2015, a equipe BOSLTER CONSULTANCY presta serviços no intuito de apoiar seus parceiros e clientes, dentre os quais se destacam a guarda e organização de arquivos físicos e digitais (GED/ECM), consultoria e digitalização de documentos. Tudo feito sempre buscando a excelência em cada processo e, principalmente, a satisfação e sucesso de seus clientes.

A **Política Corporativa de Segurança da Informação**, também referida como **PSI**, é o documento formal que orienta e estabelece as diretrizes corporativas da BOLSTER CONSULTANCY (BC) para a proteção e gestão das informações.

Esta Política estabelece os conceitos e diretrizes de segurança da informação, visando proteger as informações da ("BOLSTER CONSULTANCY" ou "Parceiros"), e de seus clientes e principalmente a proteção e a privacidade de dados dos envolvidos.

CONSIDERANDO a necessidade de estabelecer diretrizes e padrões para garantir um ambiente tecnológico controlado e seguro, de forma a promover a segurança das informações e contribuir para a continuidade do negócio desempenhado pela BOLSTER CONSULTANCY, com integridade e confidencialidade. CONSIDERANDO que a BOLSTER CONSULTANCY preza

especialmente pela preservação da sua alta credibilidade no mercado nacional e a constante preocupação com a qualidade e celeridade no desempenho de suas atividades e na prestação de serviços à sociedade como um todo e ao respeito a proteção e privacidade de dados dos titulares.

A BOLSTER CONSULTANCY estabelece como princípio norteador e objetivo de negócio o compromisso com esta Política Corporativa de Segurança da Informação, entendendo que, assim como a ética, a segurança deve ser parte fundamental da cultura e conduta da empresa.

Faz-se necessário clareza e precisão na implementação, manutenção e gerenciamento da segurança acerca dos dados e respectivas informações que a BOLSTER CONSULTANCY armazena, trata e/ou transmite, interna e externamente.

Todos os princípios e requisitos relacionados nesta política refletem o compromisso da BOLSTER CONSULTANCY com aspectos de Segurança Física, Segurança Lógica e Segurança de Pessoas.

2. OBJETIVO

Esta Política estabelece os conceitos e diretrizes de segurança da informação, visando proteger as informações da ("BOLSTER CONSULTANCY" ou "Parceiros"), e de seus clientes. Posiciona-se como documento estratégico, com vistas a promover o uso seguro dos ativos de informação da BOLSTER CONSULTANCY. Assim, deve ser entendida como uma declaração formal da Alta Administração acerca de seu compromisso com a proteção das informações sobre sua custódia, devendo ser cumprida por todos os colaboradores, estagiários e colaboradores terceirizados da BOLSTER CONSULTANCY. Onde estiver escrito BOLSTER CONSULTANCY será equivalente a terminologia "BC".
Essa política foi aprovada pela diretoria administrativa da BC, profissional com autonomia e conhecimento técnico equivalente e submetida a verificação do Encarregado de Proteção de dados e consultado para os aspectos que envolvem a proteção e privacidade de dados pessoais protegidos e regulados pela Lei federal nº 13.709/2018. A terminologia Política de segurança da Informação equivale ao termo PSI.
São objetivos da Política Corporativa de Segurança da Informação da BC:

a. Estabelecer diretrizes para a disponibilização e utilização das informações;
b. Designar, definir ou alterar papéis e responsabilidades;
c. Apoiar a implementação das iniciativas relativas à Segurança da Informação;
d. Possibilitar a criação de controles e promover a otimização dos investimentos para proteção das informações, contribuindo com a minimização dos riscos associados;

e. Estabelecer as tratativas para incidentes de segurança, bem como as penalidades aplicáveis.
f. Promover a proteção das informações, identificando e tratando riscos à tecnologia da informação e fornecendo instruções aos usuários.
g. Assegurar a confidencialidade, integridade e disponibilidade das informações, mediante utilização de mecanismos de segurança da informação, balanceando fatores de risco, tecnologia e custo;
h. Garantir a proteção adequada das informações e dos sistemas contra acesso, modificação, destruição e divulgação não autorizados;
i. Assegurar que os recursos e ativos de informação sejam utilizados apenas para as finalidades aprovadas pela Organização, estando sujeitos à monitoração e auditoria;
j. Garantir o cumprimento dessa Política e das Normas de Segurança da Informação da Organização.

A presente PSI foi baseada nas recomendações da Norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, e alinha-se com as demais leis e normas vigentes sobre o tema, assim como os objetivos e diretrizes estratégicas da BC.

A PSI busca preservar as informações e seus respectivos recursos e ativos quanto a Integridade, Confidencialidade, Autenticidade e Disponibilidade, assim considerados:

- Integridade e Autenticidade: preservar a informação em seu estado original, protegendo-a na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais durante ciclo de vida.
- Confidencialidade: preservar a informação contra acessos indevidos.
- Disponibilidade: garantia de que apenas pessoas autorizadas obtenham acesso à informação e aos recursos e ativos correspondentes sempre que necessário.

3. ABRANGÊNCIA

Esta política aplica-se a todas as áreas de negócio e operações da BC (Matriz, Unidades Próprias, Filiais e Parceiros). A observância destas diretrizes é obrigatória e reflete a Governança Corporativa acerca dos temas de Segurança da Informação Corporativa da BC.

Importância da Segurança da Informação
Após a leitura desta Política, os Integrantes, estagiários e executivos devem assinar o Contrato de Confidencialidade para confirmar que a mensagem da Política foi compreendida e se refletirá em suas atitudes.

A informação é atualmente considerada um dos recursos mais valiosos e importantes de uma empresa, contribuindo de forma direta e decisiva para uma maior e/ou menor competitividade no mercado.

Como resultado do aumento da conectividade no "Mundo Tecnológico", verificou-se concomitantemente uma maior exposição e acessibilidade facilitada, neste caso de forma negativa, levando a um crescente número de variedade de ameaças e, principalmente vulnerabilidades.

Nesse sentido, surge a necessidade de as informações serem adequadamente protegidas, independentemente da forma em que estas se apresentem (papel, meio eletrônico, vídeos, imagens, conversas, etc.) e das alterações que sofra durante todo seu ciclo de vida (passando pela elaboração, armazenamento, distribuição, compartilhamento e descarte).

É importante, portanto, que sejam aplicadas as melhores práticas de proteção para cada tipo e estágio de vida destas informações.

4. DEFINIÇÕES

Segurança da Informação – Visa a preservar as propriedades de confidencialidade, integridade, disponibilidade, não se limitando a sistemas computacionais, informações eletrônicas e/ou sistemas de armazenamento. É a área que dedica seus esforços promovendo a proteção das informações frente às ameaças de diversas naturezas.

Esta área contribui para a continuidade dos negócios, trabalhando para minimizar eventuais danos de vazamento de informações e maximizar o retorno dos investimentos frente às oportunidades de atuação para uma empresa que demonstra clareza, transparência e segurança de suas informações.

5. DIRETRIZES

A **BC** é comprometida com a observância da legislação em vigor aplicável, bem como do Código de Ética e Conduta da empresa. E para a condução de suas atividades empresariais é necessário o estabelecimento de uma Política de Segurança da Informação estruturada e clara que possibilite aderência e conformidade.

As Diretrizes constituem a base para a Gestão de Segurança da Informação e orientam a elaboração das normas e dos procedimentos internos.

A **BC** estabelece, ainda, como diretrizes a serem seguidas em seu ambiente de negócios e de atividades desempenhadas, as seguintes diretrizes organizacionais aplicáveis a **PSI**:

a. Para efeitos desta PSI, serão consideradas informações todo o conhecimento produzido como resultado do processamento de dados e informações coletadas nas atividades de seu negócio.

b. Informações produzidas ou recebidas pelos colaboradores, fornecedores e prestadores de serviço, como resultado da função exercida ou atividade profissional contratada, pertencem à BC podendo, portanto, ser monitoradas a todo o momento.

c. Processos críticos relacionados à segurança das informações, sempre que possível e aplicável, devem estar formalizados em Normas e Procedimentos Internos, tais como:
   - Classificação e Tratamento da informação;
   - Gestão e Controles de Acessos;
   - Monitoramento e Auditoria do Ambiente;
   - Gestão de Riscos;
   - Tratamento de Incidentes; etc.

d. É dever de todos os usuários de informação manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientações com a Segurança da Informação sempre que não estiver absolutamente seguro quanto à aquisição, manipulação e/ou descarte de quaisquer dados e/ou informações.

Todas as diretrizes de Segurança da Informação estarão sempre pautadas em pelo menos uma das três camadas de segurança, quais sejam: (i) Pessoas, (ii) Física, e, (iii) Lógica, conforme abaixo definido.

SEGURANÇA DE PESSOAS

As pessoas são parte fundamental da segurança da informação. Qualquer pessoa que tenha vínculo estatutário, funcional, contratual ou processual com a **SUA EMPRESA** deve entender suas responsabilidades e atuar em conformidade com as políticas da **SUA EMPRESA**. É fundamental que adotem um comportamento seguro, ético, atitudes proativas e engajadas com o objetivo de proteção das informações. Campanhas contínuas de conscientização criam condições para que a segurança da informação se torne um hábito saudável, incorporado às atividades diárias de todos os colaboradores.

SEGURANÇA FÍSICA

A segurança física é parte do contexto geral de segurança das informações. Os dispositivos de identificação e credenciais protegem a identidade do colaborador ou prestador de serviço, evitando e prevenindo acessos a locais não autorizados e/ou incidentes de falsidade ideológica, em que uma pessoa se faça passar por outra perante a **SUA EMPRESA**. Dessa forma a utilização das credenciais de identificação, são imprescindíveis a dentro do ambiente **SUA EMPRESA**, devendo ser respeitada por todos os níveis de colaboradores.

SEGURANÇA LÓGICA

Os controles de acesso lógico constituem um conjunto de procedimentos e medidas que devem ser adotados com o objetivo de proteger informações contra tentativas de acesso não autorizadas feitas por pessoas ou programas maliciosos. Os acessos e senhas pessoais são intransferíveis, na medida em que constituem mecanismos de controle, estabelecidos para viabilizar a segurança lógica da informação.

5.1. Pilares da Segurança da Informação

A **segurança da informação** é aqui caracterizada pela preservação dos seguintes pilares:

- **Confidencialidade**: A **BC** visa garantir que o acesso às informações da companhia, parceiros e de seus clientes sejam obtidos somente por pessoas autorizadas e quando o acesso de fato for necessário;
- **Integridade**: A **BC** visa garantir a exatidão e a completude das informações e dos métodos de seu processamento, bem como a integridade dos dados de clientes que estejam sob sua responsabilidade;
- **Disponibilidade**: A **BC** visa garantir que a informação esteja sempre disponível aos profissionais que de fato possuam o acesso necessário para tal e assegure que os dados estejam disponíveis de acordo com o nível de acordo de serviço contratado pelos clientes.
- **Rastreabilidade**: A **BC** visa garantir a disponibilidade de trilhas de auditoria de informações e meios de processamento, através de registos das transações e alterações realizadas em seus sistemas e aplicações.

5.2. Aspectos Gerais

- As informações (em formato físico ou lógico) e os ambientes tecnológicos utilizados pelos usuários são de exclusiva propriedade da **BC**, não podendo ser interpretado como de uso pessoal;
- As informações de clientes devem ser tratadas de forma ética e sigilosa, de acordo com as diretrizes estabelecidas pelo PPPDP – Política de Privacidade e Proteção de Dados Pessoais da **BC** e das leis vigentes;
- As informações de clientes devem ser utilizadas somente para os fins para os quais foram autorizados;
- Todos os Integrantes, estagiários e colaboradores terceirizados devem ter ciência de que o uso das informações e dos sistemas de informação podem ser monitorados, sem aviso prévio, e que os registros assim obtidos podem servir de evidência para a aplicação de medidas disciplinares;
- A **BC** mantém um compromisso com o cliente em adotar técnicas e meios de segurança mais adequados e disponíveis em relação à segurança dos dados trafegados, processados e/ou armazenados na BC.
- Os Integrantes devem possuir uma identificação única (física e lógica), pessoal e intransferível, que seja capaz de o qualificar como responsável por suas ações;
- Somente profissionais autorizados devem possuir acesso as informações da BC e de seus clientes;
- Todo processo, sempre que possível, durante seu ciclo de vida, deve garantir a segregação de funções, por meio da participação de mais de uma pessoa ou equipe;
- Os acessos devem sempre obedecer ao critério de menor privilégio, no qual os usuários devem possuir somente as permissões necessárias para a execução de suas atividades;

- Informações confidenciais como senhas e/ou qualquer informação a qual o profissional possua em seu poder durante exercício do seu cargo devem sempre ser mantidas de forma secreta, sendo terminantemente proibido seu compartilhamento;
- As responsabilidades no que tange a garantia dos pilares da segurança da informação supracitados devem ser amplamente divulgados entre as operações da **BC** fazendo valer firmemente a aplicação das diretrizes aqui descritas.
- Essa política é apoiada por um conjunto de normativas e procedimentos de segurança da informação estabelecidos pela **BC**;
- A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada e/ou para usos estatísticos sem expor os clientes de forma identificável ou para outras características de sistema disponíveis para o próprio cliente.

5.3. Gestão de Acessos e Identidade

Os acessos lógicos dos Integrantes, estagiários e colaboradores terceirizados devem ser controlados de forma que somente às informações necessárias ao desempenho de suas atividades estejam disponíveis, mediante aprovação formal.

O acesso físico dos Integrantes, estagiários, colaboradores terceirizados e visitantes aos locais que possuem recursos tecnológicos da BC, deve ser controlado, mediante aprovação formal.

5.4. Tratamento da Informação

Para assegurar a proteção adequada às informações da **BC**, deve existir um método de classificação e rotulagem da informação de acordo com o grau de confidencialidade e criticidade para os negócios da **BC**:

- A classificação deve seguir os seguintes rótulos: Restrita, Confidencial, Interna ou Pública, considerando assim, as necessidades relacionadas ao negócio;
- Todas as informações devem estar adequadamente protegidas em observância às diretrizes de segurança da informação da **BC** em todo o seu ciclo de vida, que compreende: geração, manuseio, armazenamento, transporte e descarte;
- A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada e/ou para usos estatísticos sem expor os clientes de forma identificável ou para outras características de sistema disponíveis para o próprio cliente.

5.5. Tratamento de Dados

A **BC** respeita a privacidade e protege a disponibilidade, integridade e confidencialidade dos dados pessoais, em todo o seu ciclo de vida, em qualquer formato de armazenamento ou suporte, tendo o mesmo nível de tratamento de informações confidenciais.

Todas as operações de armazenamento, tratamento e/ou transmissão, interna e externa, realizadas pela **BC** e/ou seus colaboradores, a ela vinculados a qualquer título, utilizando-se em

seus bancos de dados de: (i) dados pessoais; (ii) dados sensíveis; (iii) dados anonimizados; deverão observar a boa-fé e os seguintes princípios:

a. **Finalidade**: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

b. **Adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

c. **Necessidade**: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

d. **Segurança**: utilização de medidas técnicas e administrativas, estabelecidas pelas Políticas de Segurança da Informação da BC, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

e. **Prevenção**: adoção de medidas, estabelecidas pelas Políticas de Segurança da Informação da BC, para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

f. **Não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

g. **Responsabilização e prestação de contas**: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, estabelecidas pelas Políticas Corporativa de Segurança da Informação da BC.

A **BC** monitorará e manterá registros das operações de tratamento de dados realizadas por si e/ou por seus colaboradores, a ela vinculados a qualquer título.

A **BC**, através de sua Políticas Corporativas de Segurança da Informação e da Política de Governança de Dados Pessoais, adotará as seguintes medidas de segurança, técnica e administrativa aptas a proteger seus bancos de dados:

a. Tratamento autorizado nos termos da legislação de proteção de dados pessoais vigente;

b. Adoção de medidas de segurança para proteger os dados pessoais de acesso não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou tratamento inadequado ou ilícito;

c. Elaboração de plano de análise e resposta às violações de dados pessoais;

d. Armazenamento de modo seguro, controlado e protegido, especialmente quando se trata de dados pessoais sensíveis;

e. Processos de anonimização e pseudonimização, sempre que necessário;

f. Protocolos de criptografia na transmissão e armazenamento, quando verificado necessário;

g. Registro lógico das operações de tratamento de dados pessoais;

h. Descarte seguro dos dados pessoais ao término de sua finalidade e sua conservação de acordo com as hipóteses legais e regulatórias;

i. Transferência aos Agentes de Tratamento de modo seguro e contratualmente previsto;

j. Mapeamento e manutenção de inventário de fluxos de dados pessoais;

k. Elaboração de relatórios de impacto à proteção de dados pessoais, quando necessário;

l. Gestão e tratamento adequado de incidentes que envolvam dados pessoais.

5.6. Gestão de Riscos, Objetivos e Incidentes de Segurança da Informação

Os riscos devem ser identificados por meio de um processo estabelecido para Avaliação dos Riscos de Segurança da Informação que afetem o negócio e/ou suas estratégias, alinhados com o contexto do negócio de forma a preservar e proteger adequadamente a BC.

Os incidentes de Segurança da Informação devem ser analisados, tratados, registrados, monitorados e reportados ao solicitante e/ou dependendo do caso deve reportar também ao Comitê Conformidade.

Principais riscos relacionados

- Divulgação, alteração, adulteração e retirada não autorizadas de informações;
- Violação das informações processadas;
- Acesso às informações em desacordo com as atribuições do usuário;
- Interrupção no funcionamento dos sistemas corporativos e consequente indisponibilidade das informações;
- Atividades executadas em desacordo com políticas, Código de Conduta, normas e expectativas da organização.
- Violação aos direitos e liberdades individuais dos titulares de dados protegidos pela LGPD por meio de acesso não autorizado (terceiros), indisponibilidade de dados via ambiente de infraestrutura interna da TI (**BC**), compartilhamento junto a terceiros não autorizada, uso e finalidade estranha a compactuada no ato da coleta do dado pessoal quando do tratamento de dados pela **BC**.

Observação: O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

5.7. Treinamentos de Conscientização

A **BC** realizará treinamentos, esporádicos e permanentes para todos os seus colaboradores, independentemente do nível hierárquico e função ocupada na **BC**.

Serão identificados nas áreas e departamentos internos da **BC**, os colaboradores responsáveis por fazer cumprir todos os requisitos estabelecidos nesta **PSI**.

A BC deve realizar treinamentos de forma regular e periódica de conscientização em Segurança da Informação, e as ações devem possuir diferentes formatos e abranger diferentes públicos, podendo ser, mas não se limitando a: Treinamento Presencial ou Regular, EAD e Campanhas de Engenharia Social.

5.8. Penalidades

O descumprimento ou inobservância de quaisquer regras ou diretrizes definidas nesta **PSI** e em suas normas complementares constituirá em falta grave para todos os fins de direito, imputável à pessoa que possua vínculo, de qualquer natureza, com a **BC**, seja ele estatutário, funcional, contratual ou processual, e ao qual a **BC** responderá com a aplicação de todas as medidas cabíveis.

O uso de quaisquer informações de forma diversa ao que ela foi desenvolvida ou ainda visando obter vantagens, benefícios próprios ou para prática de atividades ilícitas acarretará na propositura das ações administrativas, trabalhistas, cíveis e/ou criminais, cabíveis, bem como na aplicação das penalidades decorrentes de tais processos, em que a **BC** cooperará ativamente com as autoridades competentes.

5.9. Responsabilidades

A despeito das responsabilidades gerais e específicas temos a seguir.

São responsabilidades gerais de todos os usuários e gestores:

- Promover a segurança das informações.
- Seguir, de forma colaborativa, as orientações fornecidas em políticas e normas de segurança em relação ao uso, armazenamento e descarte de informações.
- Utilizar de forma ética, legal e consciente os recursos de informação da BC.

São responsabilidades específicas dos colaboradores e/ou terceiros em regime de exceção, assim considerados os trabalhadores temporários e/ou prestadores de serviço):

- Entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto na PSI.

De forma geral em especial, caberá a todos os Integrantes, parceiros, estagiários e colaboradores terceirizados:

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação da **BC**;
- Realizar os treinamentos obrigatórios disponibilizados pela **BC**;
- Proteger as informações contra acessos, modificações, destruição ou divulgação não autorizada pela BC;
- Assegurar que os recursos tecnológicos, as informações e sistemas a sua disposição sejam utilizados apenas para as finalidades aprovadas pela **BC**;
- Cumprir as leis e as normas que regulamentam a propriedade intelectual;
- Não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (aviões, transporte, restaurantes, encontros sociais, etc.), incluindo a emissão de comentários e opiniões em blogs e redes sociais;
- Comunicar imediatamente à diretoria sobre qualquer descumprimento ou violação desta Política e/ou Normas ou Procedimentos, através do e-mail: administrativo@boslterbrasil.com.br, bem como reportar quaisquer incidentes de Segurança da Informação.

Cabe à área de Segurança da Informação Corporativa representada pela DIRETORIA:

- Prover ampla divulgação e revisão da Política, Normas e Procedimentos de Segurança da Informação para todos os integrantes, parceiros e colaboradores terceirizados;
- Promover ações de conscientização sobre Segurança da Informação para todos os Integrantes e Parceiros
- Propor e administrar projetos e iniciativas relacionadas ao gerenciamento da segurança da informação da **BC**;
- Convocar pessoal técnico e gerencial apto a Administrar e Monitorar os sistemas e os controles aplicados sob a gerência da diretoria (área de Segurança da Informação da **BC**).

Cabe à área de Segurança da Informação de Cloud:

- Gerenciar o acesso físico ao Data Center;
- Gerenciar o acesso lógico dos clientes de Cloud;
- Propor e administrar projetos e iniciativas relacionadas ao gerenciamento da segurança da informação aos clientes da **BC**;
- Administrar e Monitorar os sistemas e controles aplicados sob gerência da área de Segurança da Informação dos clientes da **BC**.

Cabe à área de Sustentação TI:

- Gerenciar o acesso lógico das ferramentas e sistemas da operação **BC**.

Cabe à área de Segurança Patrimonial recepcionado pela DIRETORIA:

- Gerenciar o acesso físico as dependências da **BC**.