BOZANO

INVESTIMENTOS

Política de Segurança da Informação

Válido a partir de	1º de Julho de 2017
Área Responsável	Compliance
Substitui	1.0
Versão	2.0
Destinatários	Colaboradores da Bozano

Sumário

Apresentação

Os sócios da Bozano Investimentos e suas subsidiárias, constituída no conceito de partnership, comprometem-se a garantir o cumprimento de todos os colaboradores a esta Política de Segurança da Informação, bem como prover os recursos necessários para tal.

Comitê Executivo

1. Objetivo

Definir os conceitos e diretrizes básicos quanto à Segurança da Informação, sendo os pilares: comportamento seguro e confidencialidade, controle de acesso a ambientes lógicos e físicos, e melhores práticas de segurança.

2. Abrangência e Adesão

Esta Política abrange todos os funcionários e sócios da Sociedade ("Colaboradores"), bem como terceirizados que possuam acesso a informações confidenciais da Bozano.

Os colaboradores devem aderir a esta Política através da intranet ao ingressar na companhia ou sempre que as alterações forem consideradas pela Diretoria de Compliance como relevantes e/ou demandarem obrigações adicionais aos Colaboradores, sendo obrigatória por parte de todos.

3. Conceitos

Para efeitos desta Política, considera-se:

- Ambiente físico: dependências físicas das sociedades que integram a Bozano Investimentos;
- Ambiente lógico: ambiente controlado, eletrônico, onde circulam e são armazenadas informações confidenciais, softwares e sistemas;
- Informações Confidenciais: quaisquer informações não disponíveis ao público ou reservadas e que, portanto, devem estar acessíveis somente pelas pessoas autorizadas,

pelo período necessário. Mais informações estão disponíveis na Política de Confidencialidade da Bozano;

- Segregação: garante que o acesso à informação, através de ambiente lógico ou físico da Bozano, esteja disponível apenas para as pessoas autorizadas. Mais informações estão disponíveis na Política de Segregação de Atividades da Bozano;

- Integridade: garante que a informação esteja completa e íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante seu ciclo de vida.

4. Responsabilidades

De forma geral, cabe a todos os colaboradores e prestadores de serviço:

- Conhecer e cumprir fielmente esta Política e outros documentos normativos que venham a ser divulgados;
- Evitar situações que possam caracterizar negligência ou que estejam diretamente violando o Código de Ética, as Políticas e Diretrizes Internas, ou qualquer lei ou regulamento;
- Assegurar que os recursos tecnológicos e informações disponibilizados pela Bozano sejam utilizados em conformidade às Políticas internas;
- Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizadas pela Bozano;
- Procurar o departamento de Compliance ou de Tecnologia da Informação quando julgar necessário.

5. Comportamento seguro e confidencialidade

A Bozano se compromete a adotar os padrões mais elevados em ferramentas e tecnologias de segurança da informação com o objetivo de garantir a integridade das informações e impedir: (i) acesso e transmissão de informações e arquivos confidenciais a pessoas não autorizadas; (ii) liberação de senhas e códigos de identificação de usuários; e (iii) ocorrência de ataques cibernéticos. A Bozano disponibiliza aos colaboradores as ferramentas tecnológicas necessárias para o exercício de suas funções incluindo rede interna de arquivos com backup diário e sistemas proprietários no *cloud*.

5.1 Classificação de Informações

A Bozano possui classificação das informações de acordo com o grau de confidencialidade e criticidade para a Bozano. As informações devem ser atribuídas a um proprietário, formalmente designado como responsável pela autorização de acesso às informações sob a sua responsabilidade. Todas as informações precisam estar protegidas durante seu ciclo de vida: geração, manuseio, armazenamento, transporte e descarte.

Informações Públicas: são aquelas destinadas ao público em geral de caráter informativo direcionada a investidores e *prospects*. Exemplos: informações disponíveis no website da Bozano, como relatório de gestão, *clipping information*, informações reguladas pela CVM, lâminas dos fundos.

Informações Internas: são aquelas destinadas ao uso dentro da Sociedade, só devem ser compartilhadas internamente a que tem necessidade de saber (*need-to-know*). A divulgação externa não intencional não causaria danos à Bozano, a seus clientes ou colaboradores.

Informações Confidenciais: também destinam-se a uso interno, no entanto, a divulgação seria prejudicial para a Bozano, clientes e colaboradores. Exemplos: informações sobre investidores, planos de negócio da Bozano, salário ou dividendo de colaboradores. Enfim, informações cuja divulgação só é permitida a órgãos reguladores, Receita Federal, Advogados, Contadores ou sócios.

Informações Altamente Restritas: correspondem a mais alta classificação de segurança para as informações que transitam na Bozano. Refere-se a informações cuja divulgação não autorizada provocaria danos substanciais, constrangimentos ou penalidades à Bozano, seus investidores, colaboradores ou companhias investidas dos fundos de Private Equity (ou companhia-alvo). As pessoas que tratarem essas informações têm a responsabilidade de protegê-la. Exemplos: informação antecipada e não autorizada de fusões e aquisições da Bozano, dos fundos sob gestão ou das companhias investidas, ou novos produtos e serviços.

5.2 Política de Acesso (Físico e Lógico)

A Bozano possui sistema de controle de acesso de pessoas autorizadas às dependências do escritório por cartões magnéticos com possibilidade de utilização de logs e histórico de acesso. Os setores internos possuem controle de acesso por cartões magnéticos e senhas pessoais para devida segregação das áreas de Private Equity, Asset e Fundo Quantitativo.

No ambiente lógico, a Bozano conta com infraestrutura tecnológica que permite acesso por perfil de usuário com base no princípio da necessidade da informação para execução das atividades do Colaborador. Além disso, cada colaborador possui um identificador (ID de Colaborador) registrado de forma a assegurar a responsabilidade por suas ações. Os sistemas proprietários estão integrados e contam com ferramenta de gerenciamento de controle de acesso.

O Compliance e a equipe de TI são responsáveis por operacionalizar a liberação e restrição de acesso aos Sistemas de Informação e a outros ambientes lógicos. Os acessos são periodicamente revisados pelo Compliance, que deve verificar se estão em conformidade com as atividades desempenhadas e com a Política de Segregação de Atividades.

Conforme processo interno de Recursos Humanos, o Diretor da área contratante é responsável por comunicar através do sistema Intranet qualquer movimentação de Colaborador, seja inclusão, alteração de área ou desligamento, e definir o perfil de acesso dado suas responsabilidades. A qualquer momento, o Colaborador que precisar ter acesso à informação ou ao sistema restrito deve solicitar formalmente aprovação do Compliance.

Diretriz de Controle de Acesso

- Cada colaborador é responsável pelo uso adequado das informações que possui acesso, o que inclui as senhas de acesso aos sistemas de informações e crachás de identificação.
- Em função da Política de Segregação de atividades, os acessos nas áreas são permitidos apenas a pessoas autorizadas que possuem crachá ou senha. Pessoas externas precisam estar acompanhadas por algum colaborador.

5.3 Diretriz para Senha

A senha é a chave de acesso pessoal que garante que somente pessoas autorizadas utilizem determinados dispositivos ou recursos. Por isso, cabe aos usuários alguns procedimentos de segurança.

- Não compartilhar senha, não anotar em arquivos físicos ou de fácil acesso;
- Não utilizar códigos comuns, como próprio nome, data de nascimento, nomes de parentes, números telefônicos, palavras existentes no dicionário ou números sequenciais;
- As senhas precisam ser diferentes entre si, como as de sites de Administradores, bancos, sistemas internos e externos.
- Utilize preferencialmente senhas distintas para uso corporativo e para uso pessoal;
- Troque as senhas periodicamente e sempre que suspeitar de algo.

5.4 Política de Backup

A Bozano conta com um *backup* local dos diretórios da rede realizado de segunda a sexta com possibilidade de recuperação de até 4 (quatro) meses com restrições de datas específicas. As fitas semanais e mensais são externadas e armazenadas por uma empresa especializada em armazenamento de mídia digital. Além das plataformas de *backup,* a Bozano conta com um versionamento local de aproximadamente 30 dias nos próprios servidores. As rotinas de *backup* são validadas diariamente pela equipe de TI. Os testes de "*restore*" com a validação do processo de recuperação de dados é feito mensalmente.

6. Privacidade

a. Diretriz de Utilização de E-mail

A Bozano possui servidores de e-mail configurados com camadas de proteção de segurança para prevenir vírus ou a execução de códigos maliciosos. Os usuários são frequentemente orientados a utilizar o serviço de e-mail de forma segura. Seguem diretrizes para utilização de e-mail na Bozano.

- As contas de e-mail pessoal são bloqueadas na rede da Bozano.

- O e-mail corporativo deve estar ativo sempre que o usuário estiver trabalhando no computador.
- Funcionários não podem acessar e-mail corporativo fora da empresa, por exemplo, através do celular pessoal. Apenas sócios podem ter acesso ao e-mail corporativo através de outros dispositivos.
- Não utilize contas de e-mail pessoal para comunicar-se com investidores ou parceiros, ou para enviar qualquer tipo de informação confidencial ou interna.
- Ao receber e-mails com links, verifique se o mesmo corresponde ao endereço que aparece na tela. Para tanto, posicione o ponteiro do mouse sobre o link (não clique).
- Não abra, em hipótese alguma, caso não tenha certeza da procedência do envio e da legitimidade do e-mail.

b. Diretriz de Utilização de Internet

- A área de TI deve manter os acessos à Internet configurados conforme a política de bloqueios estabelecida pelo Comitê de Compliance & Riscos Corporativos.
- A área de TI deve manter bloqueados os *cloud services* (como dropbox, onedrive e google drive). Não é permitido o uso desse tipo de serviço.
- A instalação de softwares é de responsabilidade da área de TI e bloqueada por senha.
- É proibido fazer upload ou download de softwares ou dados ilegais (“piratas”).
- Não é permitido enviar ou fazer download de músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura local ou que violem as leis de direitos autorais.
- Não é permitido o uso de compartilhadores de informações como redes Peer-to-Peer, também conhecidas como redes P2P dentro da Bozano, sendo as mesmas bloqueadas pelos serviços de firewall.
- Conforme descrito acima, somente é permitida a navegação convencional. Casos específicos que exijam outros protocolos de segurança devem ser solicitados à equipe de TI e precisam ser aprovados pelo Compliance antes da execução, com exceção das solicitações de sócios sêniores.

- A internet disponibilizada aos visitantes é acessível somente por uma rede de visitantes. Essa rede é totalmente segregada da rede interna da Bozano e não tem acesso aos servidores da Empresa.
- No caso de perda ou roubo de dispositivos móveis que contenham acesso ao e-mail corporativo, a área de TI juntamente com o Compliance devem ser comunicados imediatamente para fins de bloqueio. Nessas situações, para fins de segurança das informações, poderá ser necessário o reset do aparelho e a eliminação de todas as informações contidas no dispositivo.

c. Diretriz de Utilização da Rede Interna

- A Bozano possui segregação de pastas na rede interna. Cada área possui um perfil de acesso, e todos os perfis possuem dois níveis de segurança - leitura e edição. O diretor da área define o perfil do usuário. Qualquer alteração no perfil precisa da aprovação do Compliance.
- É proibido armazenar na rede arquivos de música, vídeos e fotos que não sejam de propriedade da empresa.
- Dispositivos externos, como pendrives e HD externos não são permitidos devido ao bloqueio das portas USB dos computadores. Em caso de necessidade para alguma atividade externa, a Bozano precisa fornecer o dispositivo e o sócio sênior da área precisa autorizar o uso.
- O usuário não deverá obter ou tentar obter acesso não autorizado a outros sistemas ou redes de computadores conectados ao serviço.
- O Acesso Remoto é permitido desde que haja uma motivação e prazo definido para o acesso e seja previamente aprovado pelo Compliance. Acesso remoto contínuo e sem aprovação do Compliance apenas para sócios sêniores e pessoas chaves do operacional dos fundos em função de contingência.
- Computadores particulares, de colaboradores da Bozano ou de visitantes, não podem ser conectados à rede interna da Bozano, salvo em situações com prévia autorização da área de Compliance e Ti.

d. Outras Diretrizes

- Não deixar papeis ou mídias removíveis da empresa contendo informações confidenciais sem o devido armazenamento quando estiver fora do local de trabalho (política de mesa limpa). Essas informações precisam estar guardadas em armários com chave.
- Informações confidenciais, quando impressas, devem ser imediatamente retiradas da impressora e trituradas, quando cabível.

7. Política de Utilização de Equipamentos

Os sócios sêniores que precisarem utilizar equipamentos pessoais para a realização de suas atividades na Bozano devem submeter os equipamentos às regras de segurança da informação definidas pela Bozano, devendo comunicar à área de TI.

8. Ações em caso de não conformidade

Os descumprimentos serão submetidos ao Diretor responsável por *Compliance* que endereçará ao Comitê de Compliance & Riscos Corporativos.

A violação comprovada a esta Política constituirá justa causa para possível aplicação de sanção disciplinar, independente das funções exercidas, e sem prejuízo das penalidades legais cabíveis, observadas as regras constantes do Contrato de Trabalho e do Acordo de Acionistas, respectivamente.

A omissão diante da violação conhecida da lei ou de qualquer disposição desta Política não é uma atitude correta e constitui uma violação ao Código de Ética e ao Acordo de Acionistas. No caso de conhecimento sobre o descumprimento a esta Política, o Colaborador deve informar tal descumprimento a qualquer membro do Comitê Executivo que tem o dever de analisar e recomendar as respectivas ações corretivas.

9. Gestão de Incidentes de Segurança

Qualquer suspeita de um incidente de segurança deve ser imediatamente reportado à área de TI e Compliance. Nenhum colaborador deverá investigar por conta própria, ou tomar ações para se defender do ataque, a não ser que seja instruído desta forma pela área de TI, que está capacitada

para conter as exposições, analisar os impactos para a Sociedade e conduzir investigações, coletando evidências para possíveis ações jurídicas.

Incidentes relevantes que possam causar prejuízos financeiros ou materiais precisam ser reportados ao Comitê Executivo para que delibere quais ações corretivas precisam ser tomadas.

10. Testes periódicos de segurança

O departamento de Tecnologia da Informação é responsável por testes periódicos e ações preventivas para detectar falhas de segurança e vulnerabilidades. O departamento de Compliance deve monitorar os resultados desses testes e manter os registros em caso de falhas e violações desta Política.

11. Treinamento

O departamento de Compliance, com apoio da área de Tecnologia da Informação, é responsável por difundir as melhores práticas dentro da Sociedade, através de treinamento disponível na Intranet para assinatura eletrônica sempre que houver uma atualização nas diretrizes de segurança ou no mínimo anualmente. Além disso, há o treinamento contínuo dos usuários com conscientização sobre as regras e procedimentos internos, bem como sobre a regulamentação relacionada.

12. Manutenção de registros da Bozano

Todas as informações e documentos na base de dados da Bozano precisam ser arquivados por período mínimo de cinco anos conforme determina a Instrução CVM nº 558/15. Os recursos computacionais da Bozano são protegidos contra adulterações com uso de senhas pessoais ao acessar dados confidenciais.