POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

2022

AZ QUEST INVESTIMENTOS LTDA.
Rua Leopoldo Couto de Magalhães Jr., 758 Cj 152
04542-000 Itaim Bibi São Paulo SP
www.azquest.com.br

FOLHA DE CONTROLE

Título	**Política de segurança da informação**
Política institucional	Política de segurança da informação
Área responsável	*Compliance* e Gestão de Riscos
Data de aprovação	30/06/2022
Data de revisão	30/06/2023
Abrangência	AZ Quest Holdings SA (CNPJ: 41.667.352/0001-82) AZ Quest Investimentos Ltda (CNPJ: 04.506.394/0001-05) AZ Quest MZK Investimentos Macro e Credito Ltda (CNPJ/MF 21.676.427/0001-84) AZ Brasile Holding LTDA (CNPJ: 37.644.295/0001-49) XP Managers Fundo de Investimento em Participações Multiestratégia (CNPJ: 32.528.586/0001-58) XP Private Equity I Fundo de Investimento em Participações Multiestratégia (CNPJ: 21.523.833/0001-07)
Procedimentos e documentos relacionados	Lei Geral de Proteção de Dados nº 13.709/2018 ("LGPD"); Instrução Normativa CVM nº 558/2015 ("ICVM 558"); Instrução Normativa CVM nº 618/2020 ("ICVM 618"); Instrução Normativa CVM nº 505/2015 ("ICVM 505"); Resolução BACEN nº 4.658/2018; PQO – Programa de Qualificação Operacional B3; e Guia de Cibersegurança ANBIMA.

Introdução

As regras descritas na integridade das normas internas e na legislação aplicável às empresas AZ Quest[1] devem ser cumpridas por todos os sócios, diretores, analistas, representantes, estagiários ou jovens aprendizes (definidos, resumidamente como "colaborador" ou "colaboradores"), de modo que todos devem ter ciência a respeito do conteúdo disposto.

Esta Política de Segurança da Informação ("Política") da AZ Quest estabelece os procedimentos e as regras a serem utilizados na gestão da segurança e da integridade do ambiente de tecnologia da informação, bem como conscientizar os colaboradores quanto aos procedimentos referentes a uso de sistemas, senhas, internet, correio eletrônico, softwares, acessos e segurança cibernética.

A presente Política garante a prestação de serviços de tecnologia da informação ("TI"), preservando a confidencialidade, a integridade e disponibilidade dos dados, definindo procedimentos para mitigar os impactos de eventuais incidentes – de modo a prevenir interrupções e assegurar a proteção dos ativos, como dados, programas e equipamentos. Além disso, é da alçada desta Política a disposição sobre a concessão e a administração de acessos de usuários a sistemas, dados e serviços na AZ Quest.

Preceitos

Os sistemas de informação, a infraestrutura tecnológica, os arquivos de dados e as informações internas ou externas da AZ Quest são vitais para o sucesso da empresa. Cada colaborador da AZ Quest tem a responsabilidade de usá-los adequadamente, protegendo sua confidencialidade e privacidade, compartilhando-os somente se necessário e na medida do que é permitido para fazê-lo.

A AZ Quest adota mecanismos de segurança cibernética com a finalidade de assegurar a confidencialidade, a integridade, a privacidade e a disponibilidade dos dados e dos sistemas de informação utilizados. São objetivos gerais da Política:

i. Proteger e respeitar a privacidade de investidores, usuários do *Website*, Parceiros, Colaboradores e outros indivíduos que mantenham uma relação comercial com a AZ Quest;
ii. Esclarecer as finalidades e as regras do tratamento de dados pessoais realizados pela AZ Quest;
iii. Identificação e avaliação dos riscos cibernéticos internos e externos;
iv. Reduzir a vulnerabilidade contra ataques cibernéticos;
v. Estabelecer medidas que serão adotadas para tratamento de incidentes cibernéticos e recuperação de dados e sistemas;

[1] O grupo AZ Quest é composto por: AZ Quest Holdings SA (CNPJ: 41.667.352/0001-82), AZ Quest Investimentos Ltda (CNPJ: 04.506.394/0001-05), AZ Quest MZK Investimentos Macro e Credito Ltda (CNPJ/MF 21.676.427/0001-84)

vi. Assegurar o controle de dados pessoais e informações confidenciais aos quais os Colaboradores tenham acesso em razão de suas atividades;
vii. Assegurar a existência de testes periódicos de segurança para os sistemas de informações, em especial para dados e documentos mantidos em formato eletrônico; e
viii. Fornecer e manter programa de treinamento de segurança de informações aos Colaboradores.

Responsabilidades

Os Colaboradores que prestam suporte de TI e administram as instalações são responsáveis pelos procedimentos de segurança dos equipamentos. Tal consentimento é coletado pelo Termo de Responsabilidade, expressando o conhecimento e a concordância aos princípios e procedimentos necessários.

As áreas de TI e *Compliance* são, coresponsáveis pela infraestrutura de tecnologia e por garantir a segurança das informações, cumprindo os critérios:

i. Monitorar as violações de segurança da informação e tomar ações corretivas em prazo razoável;
ii. Orientar os testes de infraestrutura de tecnologia e de sistemas para avaliar os pontos fracos e detectar possíveis ameaças, sugerindo medidas de aprimoramento;
iii. Assegurar que exista um processo apropriado para a comunicação dos incidentes e violações de segurança da informação detectados, independentemente dos recursos tecnológicos utilizados;
iv. Garantir a confidencialidade dos dados e da propriedade intelectual desenvolvida na AZ Quest, garantir controles de acessos;
v. Divulgar informes e treinamentos de conscientização de acordo com esta Política para com todos os Colaboradores;
vi. Manter e atualizar sistemas e dados;
vii. Promover descartes de dados e equipamentos de forma segura e manter o Relatório Anual de Riscos atualizados; e
viii. Coordenar a aplicação da legislação aplicável em caso de incidentes.

Os gestores de cada área são responsáveis pela aderência dos membros de suas equipes para com os princípios e os procedimentos desta Política.

O Comitê de *Compliance* é responsável pela aplicação desta Política, especificamente por:

i. Direcionar os esforços e recursos propostos para a segurança da informação e a proteção da privacidade;
ii. Aprovar as normas internas e suas atualizações;
iii. Acompanhar os indicadores de segurança e os incidentes reportados pelas áreas de

Compliance e, ou, de TI;

iv. Apoiar as iniciativas para melhoria contínua de medidas de proteção da informação e de privacidade, com vistas a reduzir os riscos identificados;

v. Aprovar o planejamento sobre os recursos de tecnologia, no que tange à segurança da informação e proteção da privacidade; e

vi. Delegar as funções de segurança da informação e de proteção da privacidade aos profissionais responsáveis.

Propriedade intelectual

Assim como também é detalhado nas demais normas internas que abordam o tema, é terminantemente proibido que os Colaboradores enviem, copiem, reproduzam ou imprimam arquivos utilizados, gerados ou disponíveis na rede para fins diversos aos objetivos comerciais da AZ Quest, uma vez que tais arquivos contêm informações que são consideradas como informações confidenciais.

Ademais, os Colaboradores devem se abster de utilizar *pendrives*, *hard-drives*, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na AZ Quest. Também é proibida a conexão de equipamentos ou implementação de programas e sistemas na rede da AZ Quest que não estejam previamente autorizados pelas áreas de TI e *Compliance*.

A reprodução de propriedades intelectuais apenas podem ser realizadas para execução e desenvolvimento dos negócios e dos interesses da AZ Quest. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso de maneira a evitar sua recuperação ou leitura.

Uso dos ativos, sistemas, internet e e-mail

A utilização dos ativos e sistemas da AZ Quest, incluindo computadores, telefones, *internet*, *e-mail* e demais aparelhos se destina exclusivamente para fins profissionais. O uso para fins pessoais deve ser evitado. O uso para fins pessoais nunca deve ser prioridade e, ou, prejudicar em relação a qualquer utilização profissional.

Em atendimento às normas internas, à legislação e à regulação aplicáveis, os Colaboradores estão cientes de que os sistemas de comunicação concordam e autorizam que sejam gravados, ouvidos e compartilhados, independente de ciência e anuência, não lhes dando qualquer direito

sobre o material gravado.

A AZ Quest se reserva o direito irrestrito, independente de qualquer aviso prévio, notificação ou formalidade, de inspecionar e gravar quaisquer dados contidos nos equipamentos, bem como meios de comunicação dos seus Colaboradores, realizada ou recebida, pelos meios disponibilizados pela AZ Quest para a atividade profissional de cada Colaborador. Tal atividade tem como objetivo prevenir, detectar ou minimizar impactos decorrentes do uso inadequado ou em descumprimento às normas internas, à legislação e à regulação aplicáveis.

Segurança do sistema de mensagem eletrônica

Os Colaboradores que utilizam o sistema de comunicação por meio de mensagem eletrônica estão sujeitos, aos seguintes requisitos:

i. *Firewall* de controle de borda, para limitar acesso de originadores de mensagens eletrônicas a servidores específicos, com configuração para tratar a troca;
ii. *Edge filter content*, que atua como defesa de primeiro nível, com regras *antispam*;
iii. Bloqueio de mensagens anônimas, para que sejam automaticamente rejeitadas;
iv. Ferramenta dedicada para proteção de e-mails, com detectção de *spam*, *phishing* e antivírus;
v. *Junk mail filter*: servidor de mensagens eletrônicas com filtro de categorias indesejadas, a serem automaticamente movidas a área determinadas – como lixo eletrônico, propagandas, etc;
vi. Validação de identidade, por meio de integração do servidor de e-mail ao sistema de controle de acessos da rede local, não sendo possível o acesso sem a autorização à conta de rede;
vii. Proteção antivírus, na estação de cada usuário, através de sistema de combate distribuído e gerenciado centralizadamente, com atualização automática das assinaturas de possíveis vírus. O sistema de antivírus é gerenciado através de uma console única por prestador de serviços especializado, onde existem alertas e procedimentos de automação para proteção quando se registra uma ameaça de infeção. Todos os servidores e estações de trabalho têm antivírus instalados e monitorados;
viii. Canal criptografado: a troca de comunicação é feita por meios criptografados, com a implementação de protocolo e que as mensagens são trocadas em canal que utiliza os devidos certificados digitais, garantindo a validade de remetente e destinatário, bem como a confidencialidade do conteúdo;
ix. *Backup*: diariamente, é executada cópia de segurança do servidor, para ser enviada ao armazenamento externo.

Backup

A AZ Quest conta com dois processos para cópia de segurança: (i) geração de cópia de segurança dos dados compostos por arquivos e dados, salvos na rede corporativa, com *hardware* e *software* dedicados para rotação e armazenamento na nuvem; e (ii) geração de cópias de conteúdos compartilhados pelos meios de comunicação especializados, que contam com *software* adequado.

Trimestralmente, testes de integridade das cópias armazenadas precisam ser efetuados pela área de TI, para garantir o processamento dos arquivos armazenados na nuvem, através de amostragem.

A área de TI deve compor relatório semanal a respeito do processamento das informações necessárias para identificar problemas relacionados à obtenção de cópia de segurança e deve ser enviado ao Comitê de *Compliance*. Conjuntamente, este comitê analisa todas as falhas relatadas e apontadas, bem como as ações tomadas para correção da falha.

Eventuais recuperações de dados são solicitados por e-mail para a área de TI – considerando que o armazenamento é garantido por prazo de cinco anos, conforme demanda a legislação aplicável.

Avaliação de riscos

A AZ Quest, por meio da sua área de TI, realiza avaliações de riscos regulares, compreendendo seu ambiente de segurança da informação. O objetivo de tal avaliação é de estimar a vulnerabilidade em potencial, para garantir que as medidas de segurança em uso são suficientes para reduzir os riscos a patamares aceitáveis e para estimar os investimentos relacionados à capacidade de continuidade dos negócios em caso de vulnerabilidade.

Os riscos potenciais incluem: usuários com nível de acesso inadequado, terminais desligados incorretamente, uso indevido de senha, falta de aderência aos procedimentos de segurança, falta de procedimentos de *software* antivírus, falta de controles sobre mudanças nos sistemas ou nos dados, consequências decorrentes de violações da segurança, eventos de caso fortuito ou força maior, ou riscos associados ao acesso à rede – como por ameaça interna ou externa.

Plano de respostas a incidentes

No exercício das suas atividades, a AZ Quest está sujeita a riscos cibernéticos que ameaçam a confidencialidade, integridade e disponibilidade dos dados e dos sistemas de informação utilizados. Entre os riscos mais comuns, estão:

i) *Malwares*: *softwares* desenvolvidos para corromper computadores e redes:
   a. Vírus: *software* que causa danos à máquina, rede, outros *softwares* e bancos de dados;

   b. Cavalo de Troia: aparece dentro de outro *software* e cria uma porta para a invasão do computador;

c. *Spyware*: *software* malicioso para coletar e monitorar o uso de informações; e
d. *Ransomware*: *software* malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

ii) Engenharia social: métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:
a. *Pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;
b. *Phishing*: links transmitidos por e-mails, simulando se uma pessoa ou empresa envia comunicação eletrônica oficial para obter informações confidenciais;
c. *Vishing*: simula ser uma pessoa ou empresa e, por meio de ligações telefônicas, tenta obter informações confidenciais;
d. *Smishing*: simula ser uma pessoa ou empresa e, por meio de mensagens de texto, tenta obter informações confidenciais; e
e. Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

iii) Ataques de DDoS (*distributed denial of services*) e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição. No caso dos *botnets*, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar *spam* ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços; e

iv) Invasões (*advanced persistent threats*): ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

A AZ Quest estabelece e gerencia normas internas e procedimentos para suprir a resposta a incidentes de segurança da informação, incluindo revisões de pós-incidentes de eventos, ações tomadas e planos de ação, para abordar e identificar qualquer vulnerabilidade e risco. Ademais, a AZ Quest conta com a salvaguarda reativa contra ocorrências de instrusões, para reportar e reparar ameaças.

A AZ Quest se compromete a utilizar tecnologias apropriadas para orientar e avaliar os riscos envolvendo a estrutura física e cibernética dos seus negócios, empreendendo os melhores esforços em prol da segurança. A área de TI é responsável pelos relatórios, informando, eventualmente, a natureza da violação, o sistema, as partes envolvidas, detalhes e consequências do incidente, para prevenir futuros efeitos colaterais.

Em um cenário de incidente ou em caso de substituição de prestadores de serviços relevantes, os procedimentos para garantir a continuidade dos negócios devem envolver o redirecionamento das atividades para os locais de recuperação, encerramento de operações no *datacenter* principal,

ativação de recuperação dos sistemas e recuperação de dados e reconstituição dos *datacenters* após teste para validar a qualidade dos dados recuperados. A desativação do plano de continuidade depende, necessariamente, da cessação da causa que ativou tal desastre, verificando pelos testes de qualidade e pelo funcionamento dos ambientes.

Quando aplicável, a AZ Quest informará aos reguladores, em tempo hábil, a respeito de qualquer incidente que tenha sido identificado e considerado relevante para a operação.

Ações de prevenção e proteção

Com a finalidade de mitigar os riscos cibernéticos e proteger seus sistemas, informações, base de dados, equipamentos e o andamento dos seus negócios, as áreas de TI e *Compliance* adotam as seguintes medidas de prevenção e proteção:

i) Controle de acesso adequado aos ativos, por meio de procedimentos de identificação, autenticação e autorização dos usuários, ou sistemas, aos ativos;

ii) Estabelecimento de regras mínimas (complexidade, periodicidade e autenticação de múltiplos fatores) na definição de senhas de acesso a dispositivos corporativos, sistemas e rede em função da relevância do ativo acessado. Além disso, os eventos de login e alteração de senha são auditáveis e rastreáveis;

iii) Limitação do acesso de cada Colaborador a apenas recursos relevantes para o desempenho das suas atividades e restrição do acesso físico às áreas com informações críticas/sensíveis;

iv) Rotinas de *backup*;

v) Criação de *logs* e trilhas de auditoria sempre que permitido pelos sistemas;

vi) Realização de diligência na contratação de serviços de terceiros, prezando, sempre que necessário, pela celebração de acordo de confidencialidade e exigência de controles de segurança na própria estrutura dos Terceiros;

vii) Implementação de recursos *anti-malware* em estações e servidores de rede, como antivírus e *firewalls* pessoais; e

viii) Restrição à instalação e execução de *softwares* e aplicações não autorizadas por meio de controles de execução de processos (por exemplo, aplicação de *whitelisting*).

Monitoramento

A AZ Quest possui mecanismos de monitoramento das ações de proteção implementadas, para garantir seu bom funcionamento e efetividade. Nesse sentido, a AZ Quest mantém inventários

atualizados de *hardware* e *software*, bem como realiza verificações periódicas, no intuito de identificar elementos estranhos à AZ Quest, como computadores não autorizados ou softwares não licenciados.

Além disso, a AZ Quest mantém os sistemas operacionais e *softwares* de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas. As rotinas de *backup* são monitoradas diariamente, com a execução de testes regulares de restauração dos dados.

Anualmente, as áreas de TI e *Compliance* revisam os acessos que cada colaborador tem a sistemas e informações, garantindo o *Chinese Wall* físico e virtual. Todo novo pedido de acesso precisa ser aprovado por ambas as áreas de atuação, antes da concessão. Ademais, o histórico de acessos dos usuários é controlado de forma individualizada pelo recurso que detém tais informações.

São realizados, periodicamente, testes de invasão externa e *phishing*, bem como análises de vulnerabilidades na estrutura tecnológica, sempre que houver mudança significativa em tal estrutura.

Ainda, a AZ Quest analisa regularmente os *logs* e as trilhas de auditoria criados, de forma a permitir a rápida identificação de ataques, sejam internos ou externos.

Sanções

A visualização e o compartilhamento de conteúdo, cujo cunho seja discriminatório, preconceituoso (sobre origem, raça, religião, classe social, opinião política, idade, sexo ou deficiência física), obsceno, pornográfico ou ofensivo é terminantemente proibida, conforme também descrito em demais normas internas. Na eventualidade do recebimento de mensagens com as características acima descritas, deve ser reportado o evento ao canal de denúncias.

A senha e login para acesso são pessoais e intransferíveis, não devendo ser divulgados a quaisquer terceiros. O Colaborador poderá ser responsabilizado caso disponibilize a terceiros as senhas para quaisquer fins.

Todo conteúdo que está na rede pode ser acessado pelo Comitê de *Compliance* caso haja necessidade. Arquivos pessoais não devem ser salvos em computador corporativo. A confidencialidade dessas informações deve ser respeitada e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais ou em atendimento a determinações judiciais.

Eventuais violações de segurança devem ser reportadas à área de *Compliance*, para que sejam devidamente verificadas e tratadas. As sanções decorrentes do descumprimento dos princípios estabelecidos nesta Política serão definidas e aplicadas pelo Comitê de *Compliance*, a exclusivo critério deste, garantido ao Colaborador, contudo, amplo direito de defesa. Poderão ser aplicadas, entre outras, penas de advertência, suspensão, desligamento ou demissão por justa-causa, se aplicável, nos termos da legislação vigente no País à época do fato, sem prejuízo do direito da AZ

Quest de pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio das medidas legais cabíveis.

Atualização, Disseminação de cultura e Manutenção

A Política foi aprovada internamente, e seu conteúdo é disseminado para todos os colaboradores da AZ Quest, tanto pelas vias de contato cotidianas, como no processo de treinamento imediatamente após o ingresso do colaborador, como no treinamento de atualização anual, conforme os incisos I, II e II do artigo 21 da Instrução CVM nº 558 de 2015.

Conforme detalhado a cima, anualmente, a área de *Compliance* da AZ Quest é também responsável pela elaboração do Relatório de Supervisão Baseada em Risco de PLDFTP (nos termos da Resolução CVM nº 50 de 2021), Relatório de Controles Internos (Resolução CVM nº 21 de 2021), Relatório de Prevenção à Lavagem de Dinheiro, Financiamento ao Terrorismo de Porte de armas (de acordo com Resolução nº 50 de 2021) e do Relatório de Cadastro e *Suitability* (nos termos das Resoluções CVM nº 30 e 35 de 2021), a serem elaborados até o último dia útil do mês de abril em relação às atividades desempenhadas pela AZ Quest no ano anterior.