POLÍTICA DE CIBERSEGURANÇA

Sumário

INTRODUÇÃO 2
IDENTIFICAÇÃO DE RISCO CIBERNÉTICO 3
PROGRAMA DE SEGURANÇA CIBERNÉTICA 4
AÇÕES DE PREVENÇÃO E PROTEÇÃO 5
MONITORAMENTO E TESTES 7
PLANO DE RESPOSTA 8
TREINAMENTOS 9
DISPOSIÇÕES FINAIS 10

CONTROLE DE VERSÕES	DATA	MODIFICADO POR	DESCRIÇÃO DA MUDANÇA
1.0	Novembro/2025	Jurídico	Versão Inicial

INTRODUÇÃO

O uso de tecnologias para tornar as atividades do dia a dia mais ágeis se torna essencial. Entretanto, todos os avanços tecnológicos também geram riscos de ataques cibernéticos, o que pode eventualmente ameaçar a confidencialidade, a integridade e a disponibilidade dos dados ou dos sistemas que nos utilizamos. Dentre todos os princípios norteadores da nossa conduta perante clientes, mercado e público em geral, se destacam posturas que demonstrem ações concretas, éticas e transparentes, pautadas por diligência, cuidado e integridade com a tecnologia da informação que, direta ou indiretamente, se relacionem com dados e informações de nossos clientes e/ou de pessoas relacionadas.

A presente Política de Segurança Cibernética ("Política"), elaborada em conformidade com as regulamentações do Banco Central do Brasil ("Bacen"), as diretrizes do Conselho Monetário Nacional ("CMN"), o disposto na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) e demais normas aplicáveis, tem por objetivo estabelecer regras e procedimentos para assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados para o funcionamento e desenvolvimento das atividades da Arko Consultoria E Gestão Financeira (a "Arko"), sendo implementada de acordo as recomendações e orientações do Guia de Cibersegurança da Associação Brasileira das Entidades dos Mercados Financeiros e de Capitas – ANBIMA.

Estão sujeitos aos procedimentos aqui descritos todos os diretores, sócios, funcionários, fornecedores em tecnologia da informação, terceirizados, trainees, estagiários e demais pessoas, física e/ou jurídica, que tenham acesso a dados eletrônicos da Arko ou que lhe prestem serviços em tecnologia da informação (em conjunto "Colaboradores" e em separado "Colaborador"), os quais devem conhecer integralmente as disposições desta Política, devendo zelar pelo seu fiel cumprimento, naquilo que lhes couber.

Qualquer violação às disposições desta Política será considerada um descumprimento das regras internas da Arko, e sujeitará o Colaborador às sanções disciplinares, tais como suspensão, advertência, desligamento, rescisão de contrato e /ou exclusão, de acordo com a deliberação do órgão designado pela Diretoria Executiva da Arko.

IDENTIFICAÇÃO DE RISCO CIBERNÉTICO

O uso de recursos da tecnologia da informação potencializa os riscos de ataques cibernéticos realizados por diferentes agentes (organizações criminosas ou hackers individuais, organismos de Estado, terroristas, colaboradores, competidores etc.), por diferentes motivações como, exemplificadamente, roubo, furto, adulteração ou manipulação de informações; prática de fraude, sabotagem ou exposição da Arko e/ou de empresas parceiras para obter vantagens competitivas e informações confidenciais; e/ou promover a prática de terror e disseminação do pânico e caos.

O Colaborador deve conhecer e identificar os diferentes métodos de ataques cibernéticos utilizados por invasores, em especial:

TIPO DE ATAQUE	DEFINIÇÃO
Malware	softwares desenvolvidos para corromper computadores e redes
Vírus	software que causa danos a máquina, rede, softwares e banco de dados
Cavalo de Troia	aparece dentro de outro software e cria uma porta para a invasão do computador
Spyware	software malicioso para coletar e monitorar o uso de informações
Ransomware	software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido
Engenharia social	métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito
Pharming	direciona o usuário para um site fraudulento, sem o seu conhecimento
Phishing	links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais
Vishing	simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais
Smishing	simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais
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
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
Invasões (advanced persistent threats)	ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico

PROGRAMA DE SEGURANÇA CIBERNÉTICA

A Arko, por meio da presente Política, tem como objetivo mitigar os riscos de uma ameaça cibernética com a implementação de um programa de segurança cibernética que contempla os seguintes aspectos:

a. identificação e avaliação dos riscos aos quais a Arko está sujeita;
b. estabelecimento de ações de prevenção e proteção;
c. monitoramento e testes; e
d. criação de um plano de resposta.

A Diretoria Executiva da Arko, por meio do órgão ou comitê por ela designado, será responsável por tratar e responder questões relacionadas à segurança cibernética.

Adicionalmente, para monitoramento e operacionalização de possíveis assuntos relacionados à segurança cibernética, a Arko possui um contrato de prestação de serviços com uma empresa terceirizada de tecnologia da informação ("T.I"), que assessora e dá suporte aos Colaboradores na proteção das informações de software e hardware utilizados pela Arko.

A contratação de uma empresa de T.I pela Arko passa por um processo de diligência descrito conforme política de contratação constante no Código de Ética e Conduta e, uma vez contratada, assina acordo de confidencialidade em razão da sensibilidade dos dados (pessoais e sensíveis) dos quais poderá ter acesso, sejam eles todos aqueles equipamentos, sistemas, processos ou informações utilizadas para o correto funcionamento das atividades da Arko.

No âmbito de suas atividades, a Arko atua diretamente com os chamados "Ativos Relevantes", ou seja, aqueles equipamentos, sistemas, documentos ou processos próprios, que diante de suas eventuais vulnerabilidades podem figurar como alvos em possíveis cenários de ameaças cibernéticas, uma vez que, diariamente, são tratados dados e informações a respeito de seus investidores, clientes, empresas parceiras e Colaboradores, de forma que, no caso de uma eventual ameaça cibernética, o vazamento e uso indevido desses poderia causar imensuráveis danos à Arko ou a terceiros.

A Arko utiliza, ainda, softwares licenciados e plataformas de terceiros, nos quais são realizadas atividades de backoffice e operações de clientes, que em conjunto com os Ativos Relevantes e outras tecnologias desenvolvidas internamente, integram o Quadro de Inteligência da Arko.

A utilização dos componentes e recursos do Quadro de Inteligência da Arko em computadores, telefones, internet, e-mail e demais dispositivos eletrônicos ou plataforma digital, se destina exclusiva e prioritariamente aos fins profissionais, devendo os Colaboradores evitarem o uso indiscriminado para fins pessoais. Em consonância com as disposições de Segurança e Sigilo de Informações do Código de Ética e Conduta, todos os Colaboradores devem se abster de utilizar pen-drives, HDs externos, ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de suas atividades na Arko, sendo expressamente proibido a conexão em servidores físicos ou em nuvem da Arko por quaisquer pessoas não autorizadas pela Diretoria Executiva.

AÇÕES DE PREVENÇÃO E PROTEÇÃO

Diante criteriosa análise de possíveis riscos ao Quadro de Inteligência da Arko e a potencialidade de um ataque cibernético, a Arko e seus Colaboradores devem adotar as ações de prevenção e proteção desta Política e vigilância contínua para a mitigação ou eliminação dos riscos cibernéticos e, na ocorrência de um ataque cibernético ou falha sistêmica decorrente de um ataque, devem acompanhar e realizar as ações necessárias do Plano de Resposta até a retomada da normalidade das atividades e reestabelecimento da segurança devida.

Para tanto, a Arko estabelece como primeira Ação de Prevenção aos riscos cibernéticos, a adoção de softwares de proteção atualizada contra malware e de antivírus projetado para detectar, evitar e, quando possível, limpar programas conhecidos que afetem de forma maliciosa o Quadro de Inteligência da Arko.

Todos os dispositivos eletrônicos do Quadro de Inteligência da Arko possuem software e/ou hardware, conforme cada tipo de dispositivo, firewall projetado para evitar e detectar conexões não autorizadas e incursões maliciosas. Além disso, a Arko assume o compromisso de manter os sistemas operacionais e softwares de aplicação sempre licenciados e originais, instalando as atualizações sempre que forem disponibilizadas, bem como de instruir os Colaboradores que utilizam dispositivos pessoais para desempenho das atividades a adotarem as melhores práticas de segurança cibernética.

Excepcionalmente e individualmente, conforme o caso concreto, a Arko poderá autorizar os Colaboradores a utilizarem dispositivos pessoais para o desempenho de suas atividades, que deverão atender e respeitar as regras e os procedimentos estabelecidos nesta Política e no disposto em Segurança e Sigilo de Informações do Código de Ética e Conduta, que são aplicáveis, também, a todos os Colaboradores que desenvolvam atividades em trabalho remoto.

Para todos os Colaboradores que exerçam essa modalidade de trabalho, é obrigatória a adoção das seguintes medidas:

a. manter softwares de proteção contra malware/antivírus nos dispositivos remotos;
b. relatar para a Diretoria Executiva qualquer violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações da Arko e que ocorram durante o trabalho remoto;
c. não armazenar informações confidenciais ou sensíveis em dispositivos pessoais;
d. comunicar a Diretoria Executiva a ocorrência de furto ou perda do equipamento.

A Arko manterá diferentes níveis de acesso às pastas e aos arquivos eletrônicos de acordo com as devidas segregações funções e responsabilidades de cada setor da empresa, bem como estabelecerá acesso escalonado aos sistemas do Quadro de Inteligência conforme o cargo e função de cada Colaborador, a fim de se limitar o acesso de informações confidenciais e a dados sensíveis, bem como para impedir alterações ou modificações de segurança não autorizadas que possam causar vulnerabilidade em caso de violação.

Cada Colaborador deverá possuir e manter, sob sua única e exclusiva responsabilidade, as credenciais de acesso (login e senha próprios) e autorização para acessarem os dados

contidos em computadores, e-mails ou outras tecnologias e ativos fornecidos pela Arko. As credenciais de acesso são de uso personalíssimo de cada Colaborador e são classificadas como Informação Confidencial, sendo expressamente vedada a sua divulgação para quaisquer terceiros, inclusive outros Colaboradores, anotada em papel ou em sistema visível ou de acesso não protegido.

Os Colaboradores afastados ou desligados da Arko ou que tenham mudado de função, se for o caso, terão a alteração ou exclusão imediata de suas credenciais de acesso e/ou autorizações concedidas, que serão periodicamente revisados a exclusivo critério da Arko.

Todos os programas, aplicativos, sistemas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados exclusivamente por empresa de T.I qualificada e devidamente contratada pela Arko. A empresa de T.I. poderá realizar monitoramento de quaisquer mudanças e acessos aos Ativos Relevantes. É vedada a possibilidade de os Colaboradores implantarem novos programas ou alterarem configurações, ou implantarem ou alterarem componentes físicos nos dispositivos do Quadro de Inteligência sem a permissão expressa da Diretoria Executiva. Caso haja a autorização de qualquer inclusão de novos equipamentos e sistemas em curso, a Arko garantirá a segurança de uso destes por meio de vistoria de conformidade a ser realizada pela empresa de TI contratada.

Os Colaboradores deverão, em conjunto à todos os controles previstos acima, desconfiar de e-mails com assuntos não usuais em relação ao seu desempenho de funções ou não condizentes com um ambiente idôneo de trabalho, bem como a desconfiar de e-mails solicitando dados pessoais e privados e/ou e-mails estranhos com links, hyperlinks ou anexos com as extensões .cmd; .bat; .scr; .exe; ou .ws, mesmo vindos de pessoas conhecidas uma vez que esses são alguns dos principais vetores de ataques cibernéticos.

MONITORAMENTO E TESTES

Visando o monitoramento e detecção de possíveis ameaças em tempo hábil, a Arko emprega esforços para monitorar e testar as ações de prevenção à ataques cibernéticos, a fim de reforçar os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

Desse modo, para garantir um pleno funcionamento de todos os ativos da Arko, a Área Administrativa deve manter inventários atualizados de hardware e software, bem como junto da empresa de TI contratada, identificar elementos estranhos às atividades, inclusive o acesso e/ou trabalho remoto prolongado em computadores não autorizados ou software não licenciado.

A Arko realizará o monitoramento das rotinas de backup e contingência, conforme estabelecido em política própria, além de monitorar por amostragem, de forma periódica e sempre que necessário, o histórico de acesso dos Colaboradores a sites, redes sociais, blogs, webmails, entre outros, bem como os chats de negociações, e-mails enviados e recebidos, podendo verificar, também por amostragem, as informações de acesso físico à sede ou virtual à áreas de trabalho (desktops), pastas e sistemas, que devem ser documentados pela Área Administrativa da Gestora, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento.

Ainda, serão realizados, periodicamente, testes de planos de respostas a incidentes, para que cenários de ameaça antes previstos possam ser devidamente examinados e cada vulnerabilidades seja detectada com a devida antecedência para que a Arko consiga empregar um plano de resposta imediato e efetivo, na hipótese de ocorrência um ataque cibernético.

PLANO DE RESPOSTA

Diante de uma ocorrência de algum incidente ou ataque cibernético, a Arko executará um plano de resposta, visando o tratamento e recuperação de incidentes, incluindo um plano de comunicação interna e externa, caso necessário.

Nos casos de suspeita de violação, comprometimento da rede ou de qualquer outro dispositivo da Arko, em acesso não autorizado, a Diretoria Executiva deverá ser acionada imediatamente, juntamente com a empresa de T.I contratada e o departamento jurídico para adoção de todas as medidas necessárias e aplicáveis ao caso concreto.

Na ocorrência concreta de um ataque cibernético amplo ao Quadro de Inteligência, a empresa de TI contratada e/ou outra empresa especializada a ser contratada, deverão atuar em conjunto, ou isoladamente, para resolver o incidente no menor tempo possível. Neste cenário, os Colaboradores deverão seguir as determinações da empresa de T.I até a normalização das atividades. Em se tratando de um ataque individual a um determinado Colaborador, serão disponibilizados novos equipamentos para a continuidade da prestação dos serviços por parte daquele Colaborador.

Definido o procedimento a ser realizado no caso de ocorrência de ataque cibernético, a Arko designará 1 (um) Colaborador para documentar o ocorrido e realizar o reporte, no deverão constar, no mínimo:

a) Descrição do incidente ocorrido, sua natureza, as informações acessadas e mensurar a respectiva perda;
b) Identificação das áreas e os sistemas afetados, bem como desconectar ou desabilitar os devidos sistemas;
c) Determinação os responsáveis apropriados e suas funções no cumprimento do plano de resposta;
d) Avaliação da recuperação e/ou restauração dos sistemas afetados;
e) A ocorrência ou não de notificação de todas as partes internas e externas apropriadas; e
f) Resultado total ou parcial de investigações e avaliações das circunstâncias do incidente.

Todas essas informações e relatórios gerados serão arquivados em diretórios próprios da Arko para fins de evidência em eventuais questionamentos ou demandas de terceiros.

TREINAMENTOS

Visando garantir que todos os Colaboradores exercerão suas atividades atuando nos termos e limites de todo o exposto nessa Política e o previsto na legislação aplicável, a Arko promoverá campanhas de disseminação a cultura de segurança cibernética, para conscientizar sobre os riscos envolvidos, bem como realizará treinamentos periódicos com todos seus setores, repassando, sempre que necessário, novas orientações e diretrizes.

Todos os novos Colaboradores admitidos pela Arko receberão treinamento específico no processo de *on boarding*. A todos os demais Colaboradores, os treinamentos serão realizados sempre que necessário e intensificados os Colaboradores que trabalham remotamente e para os Colaboradores que forem vítimas de incidente cibernético.

Os treinamentos estarão sujeitos a aplicação de avaliação para reforço do conteúdo, para todos os Colaboradores, podendo ser exigido aproveitamento de pelo menos 70% (setenta por cento) nos testes aplicados. A não obtenção do aproveitamento pelo Colaborador na avaliação aplicada pela Arko ou a ausência deste nos treinamentos aplicados no mesmo período de tempo, implicará automaticamente no afastamento de suas funções e o encaminhamento para a área de Recursos Humanos para as devidas implicações legais.

DISPOSIÇÕES FINAIS

A presente Política entra em vigor na data de sua publicação e vigerá por prazo indeterminado ou até ser atualizada pela Arko conforme necessidade ou alterações na legislação aplicável que demande modificações, podendo ser revista a qualquer momento, independente de comunicação ou anuência do Colaborador, sempre que a Arko entender relevante.

Todos os Colaboradores recebem uma cópia desta Política, conjuntamente às demais Políticas Internas, quando de seu ingresso na Arko, que se colocará à disposição para sanar quaisquer dúvidas referentes a esta Política.

Esta Política será publicada e estará disponível em https://arkoconsultoria.com/