Procedimento de Segurança da Informação e Cibernética

Junho de 2022.

éxes

Sumário

1. Escopo

Este documento detalha o fluxo operacional aplicável à segurança da informação e segurança cibernética(“Procedimento”).

2. Normas Relacionadas

- Lei Federal nº 13.709/2018 (“LGPD”).
- Instrução CVM nº 558/2015 (“ICVM 558”).
- Instrução CVM nº 505/2011 (“ICVM 505”).
- Código ANBIMA de Melhores Práticas de Administração de Recursos (“Código ANBIMA”).
- Manual de Segurança Cibernética ANBIMA - Versão Dezembro de 2017.
- P02-Política de Compliance e Controles Internos.
- P08-Política de BCM-Continuidade de Negócios.

3. Público Alvo

Todos os funcionários, terceiros, estagiários, sócios com funções internas, bem como eventuais conselheiros de comitês de investimento (“Colaboradores”) estão sujeitos a este procedimento.

4. Responsabilidade

A responsabilidade por segurança cibernética e da informação está a cargo da Diretor de Compliance e Risco.

5. Classificação e Tratamento das Informações

5.1. Classificação das Informações

Conforme P02-Compliance e Controles Internos, as informações armazenadas, transferidas, recebidas ou fornecidas por EXES podem ser classificadas em: **(a)** públicas; **(b)** de uso interno; **(c)** confidenciais; e **(d)** sigilosas ou estratégicas.

Qualquer informação que não esteja expressamente classificada, de modo similar ao cabeçalho desta política, ou, por sua natureza não possa imediatamente ser enquadrada em uma das demais categorias (*e.g.,* demonstrações financeiras de empresa já divulgadas ao mercado, que evidentemente são públicas), deve ser considerada confidencial pelos Colaboradores.

Dúvidas sobre a classificação de informações devem ser dirimidas pelo Diretor de Compliance e Risco.

5.2. Tratamento de Informações Confidenciais

As informações confidenciais devem ser circuladas com base no princípio *need to know.*

Assim, há concessão de acesso a informações confidenciais apenas àqueles que necessitam desse acesso para realizar suas atividades.

As regras de proteção a informações e segurança cibernética objetivam, basicamente, garantir que proteção e restrição de acesso a informações confidenciais.

Todo Colaborador deve ter em mente que há limitação ao uso de informações confidenciais, devendo estas serem usadas apenas para os fins para os quais estas foram coletadas.

Mais que regra interna, a proteção de informações confidenciais pode decorrer de dever legal. O descumprimento desta, a depender do tipo de informação, pode ser classificado como ilícito, sujeitando o Colaborador a sanções nas órbitas penal, cível ou administrativa.

Não se caracteriza descumprimento desta Política a divulgação de informações confidenciais quando em atendimento a determinações decorrentes do Poder Judiciário ou Legislativo, de órgãos fiscalizadores e reguladores, tampouco a divulgação em decorrência da natureza da atividade da EXES, tais como a divulgação a advogados, auditores e contrapartes sujeitas à mesma ou a mais restritiva legislação que EXES acerca de sigilo de dado.

5.3. Tratamento de Dados Pessoais

Em razão da atuação de EXES na distribuição de cotas de investimento de gestão própria, há cadastros de investidores e acesso a suas informações financeiras, o que, por sua vez, implica em acesso da EXES a dados de natureza pessoal e de acesso restrito de clientes.

A coleta, manutenção e gestão desses dados é sempre respaldada em exigência legal e regulatória ou em consentimento dos investidores, conforme determinação da LGPD.

Não se vislumbra, em princípio, a hipótese de coleta de dados pessoais sensíveis, na forma definida pela LGPD, salvo para cumprimento da Resolução CVM 50, no que concerne à identificação de pessoas politicamente expostas e suas partes relacionadas.

Para fins de cumprimento do artigo 35-E da ICVM 505, são considerados sensíveis dados que permitam a identificação do cliente, de suas operações e dos valores aplicados por estes em veículos e investimentos geridos por EXES.

Os times de cadastro e distribuição têm compreensão sobre a diferença entre os tipos de dados pessoais e o grau de proteção aplicável a seu tratamento. As práticas do subitem a seguir e do Item 6 levam, também, em consideração esse norte.

5.4. Risco de Vazamento de Informações

Eventual vazamento de informação, ainda que involuntário, seja decorrente de falha no processo de segurança cibernética ou de segurança da informação será: **(a)** informado à parte materialmente afetada pelo vazamento; e **(b)** tratado em estrita consonância com a previsão legal que houver a respeito.

É dever do Colaborador informar o Diretor de Compliance e Risco sobre:

- Fato, ato ou omissão que incremente o risco de vazamento de informação.
- Descumprimento, ainda que involuntário, de qualquer requisito previsto nas Seções 6 e 7, abaixo.
- Ocorrência efetiva de vazamento, caso venha a ter ciência desta.

6. Proteção e Tratamento da Informação

6.1 Princípios

A proteção e o tratamento de informação na EXES são baseados em quatro elementos:

- Confidencialidade: a informação deve ser fornecida, ainda que internamente, apenas àqueles com necessidade de a acessar (*need to know basis)*, na forma da seção anterior.
- Disponibilidade: a informação precisa estar disponível aos autorizados a acessar, inclusive no que se refere a dados inativos eventualmente armazenados por empresas responsáveis por arquivos.
- Integridade: a informação deve ser mantida em seu estado original, protegida de alterações, acidentais ou voluntárias, bem como de deterioração pelo tempo (em especial, os documentos físicos).
- Autenticidade: a EXES busca performar análise sobre a veracidade dos dados e documentos apresentados por clientes, sempre com padrões razoáveis e adequados a seu porte e atuação.

6.2 Práticas

A EXES deve garantir:

- Treinamentos, em especial para o time de distribuição e cadastro.
- Segregação de acessos e controles de acesso, com possibilidade de identificação exclusiva do Colaborador, por meio de senhas individuais e não compartilhadas.
- Critérios claros para a definição de segregação acima, de acordo com: **(a)** determinações legais ou regulatórias; e **(b)** necessidade de acesso à informação (*need to know basis*).
- Corte de acesso a diretórios, redes e nuvem no mesmo dia do desligamento de profissionais ou alteração de área.
- Contratação de provedores, *softwares* e infraestrutura tecnológica apenas de empresas renomadas e relevantes em seu mercado de atuação, com compromisso público, contratual ou dever legal de tratamento de dados em conformidade com o *General Data Protection Regulation* (“GDPR”).ou LGPD.
- Cláusula de confidencialidade ou exigência de termo nesse sentido, salvo em caso de já haver dever norma que imponha dever de sigilo (*e.g.*, sigilo profissional aplicável a escritórios de advocacia), para a atuação de terceiros que, potencialmente, tenham acesso a informações confidenciais.
- No caso de utilização sistemas eletrônicos de cadastro, trilhas de auditora que permitam o rastreamento de inclusões, alterações que, no mínimo, permitam identificar: **(a)** usuário responsável; **(b)** data e horário da alteração; **(c)** natureza do evento (inclusão, alteração, exclusão).

Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade e em sua área de trabalho (regra “mesa limpa”).

No mais, na medida em que não há acesso lógico no site EXES a clientes de distribuição, a EXES entende expressamente inaplicáveis o inciso I, alínea *a*, e o inciso II do artigo 35-G da ICVM 505. Os esclarecimentos cabíveis a clientes sobre tratamento de informações estão mencionados em P02-Compliance e Controles Internos, política pública da EXES, disponível em sua página na Internet.

7. Segurança Cibernética

7.1. Princípio

No cenário tecnológico atual, em que há extrema conexão e automatização de dados, estabelecer padrões de segurança cibernética é essencial para se garantir a segurança da informação.

Assim, esta Seção 7 complementa a anterior, com foco em configurações sistêmicas e de tecnologia.

7.2. Práticas

Estão implantados:

- Filtros de e-mail, *firewall* e antivírus.
- Emissão de ordens apenas por meios eletrônicos ou documentação escrita, garantindo que estas permaneçam gravadas, inclusive em sistemas de intermediários.
- *no-breaks, links* de internet e telefonia adequados ao porte da instituição, além de inventário de equipamento.
- Regras sistêmicas para definição de senhas (*i.e.*, número e tipos de caracteres), bem como periodicidade para a troca destas).
- Exigência de aprovação do Diretor de Compliance e Risco para a instalação de novos *softwares*, aplicativos ou ferramentas, desde que haja regular licença para uso
- Atualização constante dos sistemas operacionais e *softwares* utilizados na instituição.
- Inclusão das preocupações de segurança durante as fases de aquisição de novos *softwares*, aplicativos ou ferramentas.
- Monitoramento periódico das práticas de segurança cibernética, de modo a identificar falhas, novos riscos e incrementar os controles aplicáveis.
- Manutenção de Planilha de Controles – TI e BCM, consistente em base com inventário de equipamentos sistemas, processos críticos, planos de ação e demais informações pertinentes a segurança da informação e cibernética.

Embora não participe diretamente de iniciativas sobre o compartilhamento de informações de ameaças e vulnerabilidades, a EXES acompanha as discussões e evoluções sobre o tema.

7.3. Sistemas Críticos e Falhas Relevantes

A EXES mantém base com inventário de equipamentos sistemas, processos críticos, planos de ação e demais informações pertinentes a segurança da informação e cibernética, denominada na Planilha de Controles – TI e BCM.

Neste controle, há a identificação de computadores, redes, sistemas eletrônicos e tecnológicos considerados críticos.

Falhas relevantes nos sistemas críticos relacionados à distribuição de cotas de fundos e que tenham impacto sobre clientes deverão ser informadas ao regulador, na forma especificada na ICVM 505, a clientes atingidos e à alta administração EXES.

A relevância da falha será averiguada de acordo com: (a) volume e tipo de dado eventualmente vazado; e (b) prejuízo efetivo a clientes.

Testes para ataques serão adequados ao porte e estrutura da EXES.

No Anexo I, há exemplos de ataques cibernéticos na forma sugerida pelo Manual ANBIMA de Risco Cibernético.

7.4. Os planos de resposta a incidentes seguem a Planilha de Controles – TI e BCM, bem como as regras desta política, sem prejuízo do desenho de planos *ad hoc.* Testes e Avaliação

A EXES reavaliará, ao menos uma vez por ano a estrutura de segurança cibernética.

Tal avaliação seguirá a metodologia Abordagem Baseada em Risco, que considerará os seguintes riscos e critérios em caso de ocorrência de ataque cibernético:

- Risco de não realização de processo crítico, consoante lista constante em P08-BCM-Continuidade de Negócios.
- Risco de vazamento de dados.
- Risco de invasão a sistemas e bases.

8. Prestadores de Serviços Relevantes

Prestadores de serviços relevantes serão listados na Planilha de IT e BCM. Sua contratação seguirá os padrões definidos na P02-Compliance e Controles Internos, além de seguirem o disposto no artigo 35-J da ICVM 505, inclusive no que se refere a disposições mínimas de contrato.

9. Treinamentos

Haverá treinamentos periódicos, no mínimo uma vez por ano, sobre a P02-Política de Compliance e Controles Internos, que incluirá menção aos processos relativos à confidencialidade de informações e segurança cibernética aqui tratados.

A especificidade e o grau de detalhamento do treinamento variarão de acordo com a função exercida pelo Colaborador, sendo considerado necessário o treinamento completo para profissionais de tecnologia da informação, cadastro e distribuição e demais profissionais que acessem dados sensíveis, na forma estabelecida pela ICVM 505.

10. Manutenção e Prazo de Guarda

Todos os documentos relativos à segurança da informação e à segurança cibernética serão armazenados por, no mínimo, 5 (cinco) anos, se relativos a testes e documentos operacionais, e por prazo indeterminado, nunca inferior a 10 (dez) anos em caso de documento relacionado à atividade comercial e dados de clientes, em consonância com o prazo de prescrição do Código Civil.

11. Vigência e Atualização

Este Procedimento será revisado anualmente, sempre após o processo de avaliação mencionado na Seção 8, acima, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo.

Poderá, ainda, ser alterado a qualquer tempo em razão de circunstâncias práticas que demandem essa atualização ou por conta de determinação legal ou regulatória.

12. Sanções

O descumprimento deste Procedimento, como de qualquer regra EXES, pode gerar sanções internas, incluindo desligamento.

13. Exceções

Exceções a este Procedimento devem ser aprovadas pela Diretor de Compliance e Risco.

ANEXO I – Exemplos de Ataques Cibernéticos

Consoante Manual de Segurança Cibernética ANBIMA – Versão Dezembro de 2017[1] são exemplos de ataques cibernéticos:

- *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; e*
    - *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; 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.
- *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.*

[1] Referência original: Ver SANS, Glossary of Terms, para definições dos termos mais usados. Disponível em: https://www.sans.org/security-resources/glossary-of-terms