POLÍTICA DE SEGURANÇA CIBERNÉTICA

2023/1

Curitiba/PR

VERSÕES

Versão	Data	Responsável	Aprovação
2023/1	26/05/2023	Diretor de Risco, Compliance e PLDFT e Área de T.I.	Comitê de Compliance

1. INTRODUÇÃO

As políticas e procedimentos relativos à Segurança Cibernética estavam previstos, desde o ano de 2020, no Capítulo 12 do Manual de Compliance, Regras, Procedimentos e Controles Internos, disponível no website da gestora. No entanto, o panorama da segurança cibernética tem evoluído rapidamente, apresentando desafios cada vez mais complexos para as organizações.

Constatando o aumento significativo dos riscos cibernéticos no decorrer dos anos, a SIGA], mediante deliberação da diretoria, decidiu elaborar este manual de forma apartada e mais abrangente. Reconhecemos que a proteção dos ativos digitais e a salvaguarda das informações confidenciais são fundamentais para a continuidade dos negócios e para a manutenção da confiança dos nossos investidores e parceiros.

Este documento foi cuidadosamente desenvolvido para abordar os riscos emergentes no cenário de segurança cibernética, fornecendo diretrizes claras e procedimentos robustos para mitigar ameaças e promover práticas seguras no ambiente digital. Nosso objetivo é fortalecer a resiliência da nossa organização diante dos desafios crescentes e garantir que todas as áreas estejam preparadas para enfrentar os riscos cibernéticos de forma eficaz.

Neste manual, trataremos, em síntese, sobre as regras e procedimentos que visam proteger os sistemas de informação, prevenir ataques cibernéticos, gerenciar incidentes de segurança e promover uma cultura de conscientização e responsabilidade compartilhada. Também abordaremos as melhores práticas e os padrões reconhecidos internacionalmente para a segurança cibernética, garantindo que nossas políticas estejam alinhadas às últimas recomendações do setor.

É importante ressaltar que a segurança cibernética é uma responsabilidade de todos os colaboradores da gestora de fundos de investimento. Cada um de nós desempenha um papel fundamental na proteção dos ativos digitais e no fortalecimento da nossa postura de segurança. Portanto, encorajamos a leitura atenta deste manual e a adesão integral às políticas e procedimentos estabelecidos.

Estamos comprometidos em manter um ambiente seguro e confiável, investindo continuamente em recursos e tecnologias avançadas para mitigar os riscos cibernéticos. Este manual é uma ferramenta essencial para garantir a integridade dos nossos sistemas e dados, e para reforçar o compromisso da SIGA com a segurança cibernética.

Acreditamos que, ao adotar as práticas recomendadas neste manual, estaremos preparados para enfrentar os desafios futuros e proteger os interesses dos nossos investidores. Juntos, podemos fortalecer nossa defesa contra ameaças cibernéticas e manter a confiança de todos aqueles que contam com os nossos serviços.

2. APLICABILIDADE

Este documento abrange todas as pessoas e entidades envolvidas na operação da SIGA, incluindo colaboradores, parceiros de negócios, fornecedores e prestadores de serviços. Essas diretrizes são aplicáveis a todos os ambientes físicos e tecnológicos nos quais ocorre o processamento de dados sensíveis controlados e/ou pertencentes à SIGA.

3. RESPONSABILIDADES

São, dentre outras, responsabilidades de cada um dos quadros da SIGA os dispostos abaixo.

3.1. Colaboradores

a. Familiarizar-se com as políticas e procedimentos de segurança cibernética da empresa e seguir as diretrizes estabelecidas.
b. Utilizar senhas fortes e mantê-las confidenciais, evitando o compartilhamento não autorizado.
c. Ser consciente das práticas seguras de navegação na internet e evitar clicar em links suspeitos ou abrir anexos de origem desconhecida.
d. Relatar imediatamente qualquer incidente de segurança ou comportamento suspeito às autoridades competentes da empresa.

3.2. Diretoria de Risco, Compliance e PLDFT, Jurídico e T.I.

a. Garantir a conformidade com as regulamentações e leis aplicáveis relacionadas à segurança cibernética.
b. Monitorar e revisar regularmente as políticas e procedimentos de segurança

cibernética da empresa para garantir sua eficácia e atualização.

c. Realizar auditorias internas e externas para avaliar a conformidade e identificar possíveis vulnerabilidades.
d. Desenvolver programas de treinamento sobre segurança cibernética para os colaboradores e promover a conscientização sobre as melhores práticas.
e. Assessorar a gestora de fundos de investimento na elaboração e revisão de contratos e acordos que incluam cláusulas relacionadas à segurança cibernética.
f. Acompanhar as mudanças nas leis e regulamentações de segurança cibernética e garantir a conformidade da empresa.
g. Fornecer orientações legais sobre questões de responsabilidade, privacidade e proteção de dados relacionadas à segurança cibernética.
h. Identificar e avaliar os riscos cibernéticos que a gestora enfrenta, considerando ameaças internas e externas.
i. Desenvolver e implementar planos de mitigação de riscos cibernéticos, incluindo medidas preventivas e de resposta a incidentes.
j. Monitorar continuamente os riscos cibernéticos e atualizar as estratégias de gestão de riscos conforme necessário.
k. Estabelecer políticas e procedimentos para a classificação, armazenamento e compartilhamento seguro de informações confidenciais.
l. Implementar medidas de proteção, como criptografia, autenticação de usuários e controles de acesso, para garantir a integridade e confidencialidade dos dados.
m. Realizar auditorias de segurança da informação regularmente para identificar possíveis brechas ou vulnerabilidades.
n. Garantir a segurança dos sistemas de TI por meio da implementação de firewalls, antivírus, detecção de intrusões e outras medidas de proteção.
o. Monitorar e analisar regularmente as atividades nos sistemas para detectar comportamentos anormais ou atividades suspeitas.
p. Manter os sistemas operacionais e software atualizados com as últimas correções de segurança e patches.

4. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

A identificação e avaliação de riscos de segurança cibernética são etapas fundamentais para

garantir a proteção adequada dos ativos digitais e a mitigação eficaz de ameaças cibernéticas. Compreendendo e avaliando os riscos envolvidos, SIGA passa a ser capaz de tomar medidas proativas para implementar controles e estratégias de segurança apropriadas.

Alguns dos pontos chaves e obrigações dos responsáveis, visando a identificação e avaliação de riscos, são as seguintes:

a. Inventário de Ativos: Os responsáveis devem manter um inventário atualizado de todos os ativos de TI, incluindo hardware, software, dados e sistemas críticos. Isso inclui identificar os ativos mais valiosos e vitais para a organização.
b. Análise de Ameaças: É responsabilidade de cada colaborador identificar e avaliar as ameaças cibernéticas relevantes que possam afetar os ativos de TI da organização. Isso envolve considerar ameaças internas e externas, como malware, ataques de phishing, engenharia social, intrusões de rede e vazamentos de dados.
c. Identificação de Vulnerabilidades: Todos os colaboradores devem estar atentos às vulnerabilidades existentes nos sistemas e ativos de TI. Isso pode envolver a análise de vulnerabilidades de software, configurações inadequadas, falhas de segurança física e outros pontos de entrada para possíveis ataques.
d. Avaliação do Impacto: É fundamental que cada colaborador avalie o impacto potencial que uma violação de segurança cibernética pode ter nos negócios da organização. Devem ser considerados os danos financeiros, legais, operacionais e reputacionais que podem resultar de um incidente de segurança.
e. Estimativa de Probabilidade: Cada colaborador deve estimar a probabilidade de ocorrência de uma violação de segurança cibernética. Isso envolve considerar fatores como a sofisticação das ameaças, as medidas de segurança existentes e a conscientização dos colaboradores sobre práticas seguras.
f. Classificação de Risco: Os colaboradores devem classificar os riscos de segurança cibernética com base na combinação da probabilidade e do impacto, de acordo com suas rotinas diárias. Isso envolve a utilização da matriz de riscos estabelecida neste capítulo.
g. Priorização e Plano de Ação: É responsabilidade de cada colaborador priorizar os riscos de segurança cibernética de acordo com sua gravidade e probabilidade. Devem ser desenvolvidos planos de ação para tratar os riscos mais críticos, estabelecendo

controles, políticas e procedimentos de segurança adequados.

h. Monitoramento Contínuo: Todos os colaboradores devem implementar mecanismos de monitoramento contínuo para identificar e responder a novas ameaças e vulnerabilidades à medida que surgem. É importante manter um processo de avaliação de riscos atualizado e adaptável às mudanças no cenário de segurança cibernética.

4.1. Matriz de Riscos

A Matriz de riscos permite classificar os riscos identificados com base na sua gravidade e probabilidade. A SIGA utiliza uma matriz que utiliza as classificações "Alto", "Médio" e "Baixo" para a gravidade e probabilidade dos riscos:

Probabilidade	**Gravidade Alta**	**Gravidade Média**
Alta	Alto Risco	Médio Risco
Média	Médio Risco	Médio Risco
Baixa	Baixo Risco	Baixo Risco

Exemplificam-se fatos que podem representar riscos de segurança cibernética com diferentes níveis de probabilidade e gravidade:

Probabilidade Alta:

a. Compartilhamento inadequado de senhas entre colaboradores, aumentando o risco de acesso não autorizado às informações confidenciais.
b. Falha na implementação de patches de segurança e atualizações de software, deixando os sistemas vulneráveis a explorações conhecidas.
c. Utilização de redes Wi-Fi públicas sem proteção adequada, facilitando o acesso não autorizado aos dispositivos e dados sensíveis.

Probabilidade Média:

a. Recebimento frequente de e-mails de phishing que podem levar os colaboradores a divulgar informações confidenciais ou instalar malware em seus dispositivos.

b. Uso de dispositivos pessoais não protegidos para acessar redes corporativas, aumentando o risco de infecção por malware ou vazamento de dados.
c. Compartilhamento de arquivos confidenciais com parceiros de negócios sem as devidas medidas de segurança, aumentando o risco de acesso não autorizado.

Gravidade Alta:

a. Acesso não autorizado a informações financeiras dos clientes, resultando em perda financeira significativa para a organização e danos à reputação.
b. Ransomware que criptografa os dados críticos da organização, resultando em paralisação dos sistemas e exigência de pagamento de resgate.
c. Vazamento de informações confidenciais dos clientes, violando a privacidade e regulamentações de proteção de dados.

Gravidade Média:

a. Interrupção temporária do acesso aos serviços online da organização devido a um ataque DDoS.
b. Roubo de informações de login de colaboradores, permitindo acesso não autorizado a sistemas internos, mas com menor impacto financeiro ou operacional.
c. Exposição de informações internas não críticas devido a uma brecha de segurança.

5. MITIGAÇÃO DE RISCOS

Algumas das medidas utilizadas para o tratamento de Riscos utilizadas pela são:

a. Implementar autenticação em dois fatores para todos os colaboradores como medida adicional de segurança.
b. Realizar auditorias de segurança regulares para identificar e corrigir vulnerabilidades nos sistemas críticos.
c. Estabelecer backups frequentes e testes de recuperação de desastres para garantir a disponibilidade e integridade dos dados.
d. Realizar treinamentos regulares de conscientização sobre segurança cibernética para

todos os colaboradores.

e. Reforçar políticas de senhas fortes e atualização regular das mesmas.
f. Implementar firewall de rede e monitoramento de tráfego para detectar e bloquear atividades suspeitas
g. Manter sistemas e softwares atualizados com as últimas correções de segurança.
h. Implementar políticas de acesso e segregação de funções para limitar o acesso aos dados sensíveis.
i. Realizar revisões periódicas de permissões de acesso a sistemas e aplicativos para garantir que sejam apropriadas e atualizadas.
j. Implementar sistemas de detecção de intrusões (IDS) e prevenção de intrusões (IPS) para identificar e responder a atividades maliciosas em tempo real.
k. Estabelecer uma equipe dedicada a monitorar e analisar os logs de segurança, identificando padrões suspeitos e tomando ações corretivas.
l. Realizar testes de penetração (pentests) regulares para identificar vulnerabilidades nos sistemas e aplicar correções necessárias.

Sem prejuízo, com o objetivo de se assegurar o cumprimento das políticas de confidencialidade e segurança da informação, serão adotados, entre outros, os seguintes pontos preventivos:

a. Identificação e Classificação da Informação: O colaborador que receber ou tratar uma informação deverá classificá-la em uma dentre as quatro definições expostas neste documento, de acordo com as necessidades dos negócios e os possíveis impactos no caso de utilização indevida.
b. Gestão de Informações Confidenciais: As informações confidenciais deverão ser identificadas desta maneira em qualquer meio de comunicação (e-mails, memorandos, documentos, arquivos físicos ou eletrônicos). As informações confidenciais serão salvas em HD externo segregado ou dispositivo de armazenamento em nuvem, com limitação e senhas de acesso. Os e-mails serão protegidos. Eventual documento disponibilizado a terceiros deve indicar a sua qualificação e editada com marca d´água ou carimbo especial. C.
c. Salvaguarda da Informação: Toda informação terá o ciclo de vida definido pelas seguintes etapas: geração, manuseio, armazenamento e descarte. O tempo de cada

uma das etapas deverá ser de conhecimento do colaborador, que terá a liberdade de consultar a Diretoria de Risco, Compliance e PLDFT em caso de eventuais dúvidas. Por fim, o descarte deverá ser feito por técnico de Tecnologia da Informação (TI), que não poderá ter acesso às informações e, portanto, será acompanhado durante o processo. Em caso de documentos em papel, estes deverão ser incinerados ou fragmentados.

d. Controle de Acessos: Os acessos físicos e digitais dos documentos serão rastreados, a fim de garantir a possibilidade de auditoria, que poderá identificar individualmente cada colaborador que acessou as informações.
e. Quaisquer riscos e incidentes deverão ser, imediatamente, reportados ao Diretor de Risco, Compliance e PLDFT. O plano de contingência e de continuidade dos sistemas e serviços implantados deverá ser testado semestralmente, com o objetivo de se minorar quaisquer riscos de perda de informações, confidencialidade, integridade e disponibilidade da documentação, assim como o backup.

Em respeito aos artigos 22 e 23 da Resolução CVM nº 19/2021, os documentos e informações exigidos pela CVM serão mantidos pelo prazo mínimo de cinco anos, salvo por determinação expressa em sentido contrário pelo órgão, bem como toda a correspondência, interna e externa, todos os papéis de trabalho, cálculos que fundamentaram a cobrança de taxa de performance de seus clientes classificados como investidores profissionais, quando for o caso, relatórios e pareceres relacionados com o exercício de suas atividades e os estudos e análises que fundamentaram as orientações, recomendações ou aconselhamentos.

Todos os e-mails e arquivos serão armazenados em um file server com altos padrões de segurança e ética, possibilitando controle de acesso e rastreamento de uso dos arquivos por usuário, o que garante a preservação de informações confidenciais e a restrição de acesso aos arquivos sensíveis.

O file server, que fica hospedado internamente, também possui, como medida de segurança adicional, um sistema de cópia incremental para um repositório na nuvem com periodicidade semanal.

Toda a base de dados conta com a realização de backups simultâneos que ficam armazenados na nuvem e que permitem, em caso de falhas operacionais, recuperação de dados e arquivos.

O file server é acessado, pelos colaboradores, mediante login com usuário e senha

próprios, tendo os usuários permissões diferenciadas de acordo com as funções e atividades desempenhadas por cada profissional. Os diferentes níveis de permissão viabilizam melhor controle de acesso e de reprodução dos dados e arquivos pelos profissionais.

Por fim, de forma não taxativa, as seguintes condutas devem ser observadas: (i) Os colaboradores devem evitar circular em ambientes externos à SIGA com cópias (físicas ou digitais) de arquivos contendo informações confidenciais, devendo essas cópias ser mantidas com senha de acesso. (ii) O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação, sempre com a orientação do superior hierárquico. (iii) As informações que possibilitem a identificação de um cliente da SIGA devem se limitar a arquivos de acesso restrito e apenas poderão ser copiadas ou impressas se forem para o atendimento dos interesses da entidade ou do próprio cliente. (iv) Os colaboradores devem estar atentos a eventos externos que possam comprometer o sigilo das informações da SIGA, como, por exemplo, vírus de computador, fraudes, entre outros. (v) Assuntos confidenciais não devem ser discutidos em ambientes públicos ou locais considerados expostos.

6. PLANO DE AÇÃO PARA RESPOSTAS A INCIDENTES E GESTÃO DE RISCOS CIBERNÉTICOS

Este capítulo tem como objetivo estabelecer diretrizes para a resposta efetiva a incidentes e a gestão de riscos cibernéticos na gestora. Ele deve ser implementado e seguido por todos os colaboradores, e visa garantir a comunicação imediata, definição de papéis e responsabilidades, classificação dos incidentes, implementação de medidas de contingência e retorno às operações normais após a resolução dos incidentes.

6.1. Comunicação

a. Definiram-se mecanismos de comunicação imediata à todos os colaboradores relevantes em caso de incidentes;
b. Envio de e-mails e alertas de emergência;
c. Reuniões Emergenciais do Comitê de Compliance;
d. Designação de um colaborador do departamento de Tecnologia da Informação (TI) como ponto focal interno responsável pela coordenação e comunicação dos

incidentes cibernéticos dentro da empresa.

6.2. Medidas de Contingência

Exemplificativamente, a depender da gravidade ou extensão do incidente, tais medidas de contingência poderão ser aplicadas:

a. Restrição de Acesso Físico aos Escritórios:
    a. Acionamento de plano de trabalho remoto para todos os colaboradores, com acesso seguro aos sistemas e dados da empresa por meio de conexões VPN.
    b. Configuração e teste antecipadamente a infraestrutura necessária para o trabalho remoto, como a disponibilidade de laptops e acesso à internet.
    c. Comunicação aos colaboradores sobre o acionamento do plano de trabalho remoto e fornecer instruções claras sobre como acessar os recursos necessários.

b. Indisponibilidade de Sistemas Críticos:
    a. Ativação dos sistemas alternativos ou de backup que possam ser ativados em caso de indisponibilidade dos sistemas críticos.
    b. Início de processos para a migração e restauração dos dados e aplicações nos sistemas alternativos.

c. Ataques de Malware ou Ransomware:
    a. Isolamento imediato dos sistemas afetados para evitar a propagação do malware ou ransomware.
    b. Notificação à equipe de resposta a incidentes e os responsáveis pela segurança cibernética para iniciar a análise e contenção do ataque.
    c. Restauração dos sistemas a partir de backups seguros e confiáveis, garantindo que os dados não tenham sido comprometidos.

d. Vazamento de Dados:
    a. Identificar a origem e a extensão do vazamento de dados.
    b. Notificar imediatamente os departamentos responsáveis, como Compliance

e Jurídico, para cumprir com as obrigações legais e regulatórias.

c. Implementar medidas corretivas para conter o vazamento.

7. DISPOSIÇÕES FINAIS

Este documento não aborda todas as possíveis contingências e/ou planos de ação necessários, tratando-se de material explicativo e de diretrizes de ação. Todo o exposto nesta política deve ser interpretado em conjunto com o Código de Ética e com as disposições do Manual de Compliance, Regras, Procedimentos e Controles Internos, ambos disponíveis no website da SIGA (www.sigafinance.com.br).

O desrespeito a quaisquer das regras da SIGA resultarão em Processo Administrativo Interno, podendo imputar sanções internas, de acordo com deliberações da Diretoria, incluindo desligamento. Eventuais medidas legais poderão ser tomadas pela entidade em face do infrator.

Quaisquer alterações legais ou normativas expedidas pelos órgãos regulamentadores e competentes serão aplicadas imediatamente a esta política, e todos os colaboradores serão imediatamente alertados de eventuais mudanças.

Em caso de dúvidas de interpretação ou eventuais antinomias entre as regras aqui dispostas e outras vigentes na entidade, deverá haver consulta imediata ao Diretor de Risco, Compliance e PLDFT, por intermédio do e-mail matheus.cardoso@sigafinance.com.br ou pelo telefone (41) 3044- 7464.