Política de Segurança Da Informação

SIRIUS finance

SUMÁRIO

1. OBJETIVO

A Política de Segurança da Informação da Sirius ("Política") visa garantir a proteção e a manutenção da integridade das informações de sua propriedade e/ou sob sua guarda, definindo as regras que representam, em nível estratégico, os princípios fundamentais incorporados pela Sirius para o alcance dos objetivos de segurança da informação. As normas e procedimentos de segurança da informação serão ser criados com base nas Diretrizes e deverão ser cumpridos pelo Pessoal Obrigado.

2. VIGÊNCIA

A Política entrará em vigor na data de sua aprovação e permanecerá em vigor por prazo indeterminado, devendo ser revisada pela sua área proprietária, e submetida à aprovação pelo Conselho de Sócios, pelo menos, uma vez ao ano.

A Política poderá ser revisada em períodos inferiores a um ano, nos casos em que houver alteração das práticas de negócios da Sirius que justifiquem tal revisão.

3. DEFINIÇÕES

Sócio controlador: O sócio ou grupo de sócios, vinculado(s) por acordo ou sob controle comum, que exerça(m) o poder de controle, direto ou indireto, sobre sociedade.

Companhia: Sirius Finance Ltda.

Criticidade: Caracterizada pela sensibilidade da informação e pelos possíveis impactos e danos que podem ser causados à Sirius em hipóteses como o seu vazamento e/ou o mal-uso, dentro ou fora do ambiente da Sirius.

Diretrizes: São os seguintes principais objetivos de segurança que orientam os esforços da Sirius para garantir a proteção da informação: (i) garantia da confidencialidade, proteção e disponibilidade da informação produzida ou recebida pela Sirius; (ii) garantia da integridade e confidencialidade dos registros contábeis, financeiros e de clientes da Sirius; e (iii) garantia da preservação da imagem e credibilidade da Sirius.

Sirius: A Companhia, seu Sócio Controlador e suas Controladas e Coligadas constituídas no Brasil, consideradas em conjunto.

Pessoal Obrigado: (i) Sócio Controlador da Companhia, se houver; (ii) administradores das sociedades da Sirius; (iii) membros de quaisquer órgãos estatutários das sociedades da Sirius com funções técnicas ou consultivas; e (iv) funcionários, colaboradores, estagiários, prestadores de serviços e prepostos das sociedades da Sirius.

Proprietário da Informação: Sócio ou consultor da Sirius, responsável (i) pela aprovação, revisão e cancelamento de autorizações de acesso a determinado conjunto de informações pertencentes às sociedades

da Sirius ou sob a sua guarda; e (ii) pela definição dos controles pertinentes às informações sob a sua administração e gerência.

4. NORMAS DE SEGURANÇA DA INFORMAÇÃO

As normas de segurança da informação especificam, no plano tático, os controles que deverão ser implementados para o alcance dos objetivos de segurança da informação definidos nesta Política. As normas devem abranger disposições sobre questões como, por exemplo:

i. o uso aceitável dos ativos da Sirius;

ii. o controle de acesso à informação;

iii. o controle de acesso físico;

iv. a classificação da informação; e

v. o monitoramento e gestão de incidentes relacionados ao uso e segurança da informação.

5. PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Os procedimentos de segurança da informação são, no nível operacional, normas fixadas para garantir a correta aplicação desta Política na Sirius.

6. REGRAS GERAIS

As informações e os ambientes tecnológicos utilizados por seus respectivos usuários são de exclusiva propriedade da Sirius, sendo vedada a sua utilização para fins pessoais ou quaisquer outros fins, ainda que comerciais, que não os estabelecidos nos termos das normas e procedimentos da Sirius.

O Pessoal Obrigado deve ter ciência de que o uso das informações e dos sistemas de informação pode ser monitorado, e que os registros assim obtidos serão utilizados para detecção de violações da Política, normas e procedimentos de segurança da informação.

As regras relacionadas à segurança da informação devem ser estabelecidas em normas e procedimentos específicos, acessíveis e efetivamente difundidos a todo o Pessoal Obrigado.

Sem prejuízo do disposto nesta Política, as Pessoas Obrigadas deverão observar, ainda, as disposições contidas nas leis, normas e regulamentos aplicáveis (*e.g.*, Instruções nº 380/2002, 461/2007, 558/2015 e 542/2013 da Comissão de Valores Mobiliários; Resoluções do Conselho Monetário Nacional do Banco Central do Brasil nº 3.380/2006, 2.554/1998; Lei Complementar nº 105/2001; Lei nº 12.965/2014; e Programa de Qualificação Operacional BM&FBOVESPA).

7. CLASSIFICAÇÃO DA INFORMAÇÃO

Para assegurar a proteção adequada das informações, a Sirius classificará a informação de acordo com o seu grau de confidencialidade e Criticidade.

As informações de cada área de negócio da Sirius devem ser atribuídas ao Proprietário da Informação.

8. CONTROLE INTERNO DO ACESSO À INFORMAÇÃO

O acesso às informações e aos ambientes tecnológicos da Sirius deve ser permitido apenas às pessoas autorizadas pelo Proprietário da Informação, de acordo com o princípio do menor privilégio (apenas o necessário para o desempenho de seu trabalho), a segregação de funções conflitantes e considerando a classificação da informação.

O controle de acesso aos sistemas deve ser formalizado e deve contemplar, no mínimo, os seguintes controles:

i. a utilização de identificadores (credencial de acesso) individualizados, de utilização monitorada e passíveis de bloqueios e restrições (automatizados e manuais), seguindo o princípio do menor privilégio e de segregação de funções;

ii. a remoção de autorizações dadas a usuários afastados ou desligados da Sirius, ou ainda que tenham mudado de função; e

iii. a revisão periódica das autorizações concedidas.

As regras de armazenamento, atribuição, alteração, manutenção e uso de senhas devem ser definidas por meio de normas e procedimentos específicos.

9. PARTES EXTERNAS

Os contratos celebrados entre a Sirius e as empresas prestadoras de serviços com acesso às suas informações e/ou ao seu ambiente tecnológico devem conter cláusulas com o objetivo de preservar a confidencialidade entre as partes e assegurar, no mínimo, que os profissionais sob sua responsabilidade:

i. observem e cumpram com essa Política, bem como as demais leis, regulamentos e normas aplicáveis (*e.g.*, que tratem de aspectos atinentes a propriedade intelectual e preservação do sigilo bancário);

ii. assegurem que as informações, os sistemas e o ambiente tecnológico à sua disposição sejam utilizados apenas para as finalidades autorizadas pela Sirius; e

iii. comuniquem imediatamente à área de Segurança da Informação da Sirius qualquer descumprimento ou violação a esta Política.

10. OBRIGAÇÕES

Compete ao Pessoal Obrigado:

i. cumprir fielmente a Política, as normas e os procedimentos de segurança da informação da Sirius, bem como as demais leis, regulamentos e normas aplicáveis (*e.g.*, que tratem de aspectos atinentes a propriedade intelectual e preservação do sigilo bancário);

ii. proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados pela Sirius;

iii. assegurar que os recursos tecnológicos sejam utilizados apenas para as finalidades autorizadas pela Sirius;

iv. não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas

(aviões, quaisquer outros meios de transporte, restaurantes, encontros sociais etc.) ou com terceiros não autorizados estranhos à Sirius;

v. não emitir comentários e opiniões relacionados às atividades da Sirius em ferramentas de mensagens instantâneas, portais, blogs e redes sociais e afins;

vi. nunca compartilhar ou divulgar senhas de usuário, sendo sabido que a senha é individual, intransferível e de responsabilidade do usuário; e

vii. comunicar imediatamente à área de Segurança da Informação da Sirius qualquer violação desta Política e/ou das demais normas e procedimentos de segurança da informação.

Compete ao Conselho de Sócios:

i. aprovar a Política de Segurança da Informação e suas revisões;

ii. quando demandada, tomar as decisões administrativas referentes aos casos de descumprimento da Política e/ou de suas normas; e

iii. analisar e aprovar os casos de exceção, nos termos desta Política.

Compete ao sócios e consultores, funcionários e às demais áreas da Sirius:

i. cumprir e garantir o cumprimento desta Política, além das outras normas e procedimentos relacionados à segurança da informação;

ii. assegurar que as suas equipes tenham acesso e ciência das regras contidas nesta Política, das normas e dos procedimentos de segurança da informação;

iii. informar, de imediato, à área de Segurança da Informação a cessão de necessidade de acessos de partes externas (empresas contratadas pela área), com acesso à informação da Sirius;

iv. comunicar imediatamente à área de Segurança da Informação os casos de violação de segurança da informação;

v. assegurar que a gestão da segurança da informação esteja em conformidade com as Diretrizes;

vi. assegurar que os recursos necessários para a gestão da segurança da informação estejam disponíveis; e

vii. promover a melhora contínua e dar suporte à área de Segurança da Informação, incluindo a área de Tecnologia da Informação (TI).

Compete à área de Compliance:

i. guardar todos os Termos de Responsabilidade, disponível no Código de Conduta e Ética, assinados pelo Pessoal Obrigado, documento em que eles atestam a ciência sobre todos os aspectos tratados nessa Política e a sua estrutura de funcionamento;

Compete à área de Recursos Humanos:

ii. disponibilizar a Política e as normas de segurança da informação para o Pessoal Obrigado;

iii. dar suporte ao Proprietário da Informação, quando demandada, na identificação dos papéis dos funcionários e estagiários para o processo de definição das regras de segregação de funções;

iv. garantir a guarda dos documentos privados e confidenciais de pessoa natural, respeitando o direito à privacidade do indivíduo, em conformidade com as classificações de confidencialidade e Criticidade;

v. informar, de imediato, à área de Segurança da Informação todos os desligamentos, afastamentos, licenças, férias e modificações no quadro funcional da Sirius; e

vi. comunicar imediatamente à área de Segurança da Informação os casos de violação de segurança da informação.

Cabe à área de Tecnologia da Informação (TI):

i. operacionalizar as normas e procedimentos relacionados a esta Política, por meio dos recursos de TI, conforme orientação da área de Segurança da Informação;

ii. assegurar que as informações tenham cópias de segurança (backup), que os acessos lógicos e físicos aos ativos de tecnologia da informação sejam registrados, como por exemplo, as trilhas de auditoria, *logs* e acesso físico às áreas restritas; e

iii. comunicar imediatamente casos de violação de segurança da informação à área de Segurança da Informação, independentemente do caso ter relação com a tecnologia ou não.

Compete à área de Segurança da Informação:

i. propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação da Sirius;

ii. propor o planejamento e a alocação de recursos financeiros, humanos e de tecnologia, no que tange à segurança da informação;

iii. assegurar que o Pessoal Obrigado esteja consciente das Diretrizes e/ou das normas e procedimentos desta Política, com base na educação, através de ações de conscientização como palestras, workshops, fóruns, minicursos, termos etc.;

iv. estabelecer procedimentos relacionados a instrumentação e operacionalização da segurança da informação da Sirius; e

v. apresentar nas reuniões dos Comitês de Sócios avaliação sobre o desenvolvimento das atividades, propor melhorias e tratar dos demais assuntos relacionados à segurança da informação.

11. DESCUMPRIMENTO DA POLÍTICA

Na hipótese de violação desta Política ou das normas de segurança da informação, os Sócios, com o apoio das áreas de Jurídico, *Compliance* e Recursos Humanos, determinarão as sanções administrativas que serão aplicadas ao infrator, sendo que:

i. para as Pessoas Obrigadas, a advertência formal será realizada nos casos de menor gravidade e o desligamento do infrator dos quadros da Sirius poderá ser realizado para os casos de maior gravidade; e

ii. para os prestadores de serviços e prepostos, poderá ser determinada a rescisão imediata do respectivo contrato estabelecido com o infrator.

Sem prejuízo das sanções administrativas mencionadas acima, a Sirius poderá, em quaisquer circunstâncias, adotar as medidas legais cabíveis para a responsabilização criminal e cível do infrator.

12. EXCEÇÕES

Para os casos de exceção ao cumprimento das regras previstas nesta Política, nas normas e nos procedimentos de segurança da informação, a área de Segurança da Informação apresentará pedido de exceção aos Sócios com as razões que o fundamentam, sendo necessário a aprovação de sócios que detenham o controle de, no mínimo, dois terços do capital social da Sirius.