PORTOFINO
Multi Family Office

Política de Segurança da Informação e de Proteção de Dados

Área de Compliance

Versão 2024.1

Data de início da vigência: 27.06.2024

Índice

I – Controle de versão 3
II – Documentos vinculados 4
III – Sumário executivo 5
IV – Introdução 6
V – Princípios básicos da segurança da informação 6
VI – Definições da LGPD 7
VII – Classificação e ciclo das informações 7
VII.1. Classificação das informações conforme a confidencialidade 7
VII.2. Ciclo das informações 9
VIII – Conscientização da importância da política de segurança da informação e da proteção de dados 9
VIII.1. Treinamento, compreensão e adesão da política 10
VIII.2. Riscos de não cumprimento desta Política 10
IX – Programa de segurança da informação e de proteção de dados 12
IX.1. Identificação / avaliação de riscos 12
IX.2. Ações de prevenção e proteção 12
IX.3. Monitoramento e testes 13
IX.4. Plano de resposta 13
IX.5. Reciclagem e revisão 14
X – Governança 14
X.1. Comitê de segurança da informação 14
X.2. Responsabilidades 15
XI – Disposições gerais 15
XI.1. Documentação 16
XI.2. Infrações 16
XI.3. Situações não previstas nesta política 16
XI.4. Treinamento e disseminação do conteúdo 16
XI.5. Ciência dos colaboradores quanto ao monitoramento de atividades 16
XI.6. Atualização da política 17
XI.7. Vigência 17
Anexo I – Regras de manuseio, armazenamento, transporte e descarte das informações 18
A.I.1. Política de e-mails 18
A.I.2. Política de senhas 19
A.I.3. Política de internet 19
A.I.4. Política de uso da estação de trabalho 19
A.I.5. Política social 20
A.I.6. Política de uso de celulares (voz) 20
A.I.7. Política de uso de aplicativos de mensagens instantâneas 21
A.I.8. Política de segregação de atividades 21
A.I.9. Política de manuseio, armazenamento, transporte e descarte de arquivos 22
A.I.10. Avisos importantes em apresentações 23
Anexo II – Monitoramento e controle de manuseio, armazenamento, transporte e descarte de informações e dados 24
A.II.1. Política de monitoramento de atividades 24
Anexo III – Gestão de incidentes de segurança da informação e de proteção de dados 25
A.III.1. Política de gestão de incidentes de segurança 26
A.III.2. Incidentes de proteção de dados pessoais 26
Anexo IV – Procedimentos relativos a dados pessoais 28
A.IV.1. Direitos de clientes, colaboradores e terceiros relativos ao tratamento de dados pessoais 28
A.IV.2. Procedimentos relevantes passíveis de solicitação pela ANPD 29
Anexo V – Resumo comparativo entre Códigos maliciosos 30
Anexo VI – Autoridades e entes e órgãos reguladores e autorreguladores pertinentes 31
Anexo VII – Exemplos de Normas e diretrizes externas cujos dispositivos parcial ou totalmente aplicáveis 32
Anexo VIII – Glossário 34

I – Controle de versão

Versão	Data	Nome	Ação (Elaboração, Revisão, Alteração e Aprovação)	Conteúdo
024.1	27.06.2024	Portofino Gestão	Aprovação	Aprovação da diretoria Entrada em vigor: 27.06.2024

II – Documentos vinculados

São documentos vinculados a esta Política:

Documentos	Finalidade
Plano de Continuidade de Negócios	• Definir as regras aplicáveis com base na estrutura da **Portofino**; e • Assegurar que todos conheçam o Plano de Continuidade de Negócio.
Política de Privacidade	• Descreve os direitos das pessoas naturais em relação aos seus dados pessoais e dá publicidade aos Clientes e colaboradores quanto ao tratamento por parte da **Portofino** e as respectivas finalidades.

III – Sumário executivo

Objetivos desta Política:

- Proteger os Clientes e a **Portofino**, inclusive quanto às suas imagens, e as informações pertencentes a ambos quando do seu tratamento;
- Garantir a continuidade dos negócios e das operações de forma que não haja interrupção dos serviços prestados aos Clientes da **Portofino**;
- Reduzir os riscos de fraudes, espionagens, sabotagem, vandalismo, problemas causados por vírus, erros, uso indevido e roubo de informações, bem como diversos outros problemas que possam comprometer os princípios básicos da segurança da informação;
- Garantir o cumprimento da Lei Geral de Proteção de Dados no que concerne a Segurança da Informação; e
- Definir as regras aplicáveis com base na estrutura da **Portofino**.

Áreas de atuação da Portofino:

Área	Atua
Gestão de Carteiras	Sim
Gestão de Patrimônio Financeiro	Sim
Distribuição de Fundos Próprios	Sim
Administração Fiduciária de Fundos	Sim
Serviços Pessoais, Patrimoniais e de Negócios	Sim

Produtos:

- Carteiras Administradas;
- Fundos de Investimentos;
- Gestão de Patrimônio Financeiro; e
- Serviços de Assessoramento em Assuntos Pessoais, Patrimoniais e de Negócios.

Diretor Responsável por esta Política:

- Diretor de Compliance.

IV – Introdução

Informação compreende qualquer conteúdo ou dado que tenha valor para uma determinada empresa ou pessoa e que possa ser armazenado, transferido ou manipulado de algum modo, servindo a determinado propósito (por ex. tomada de decisão etc.). Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Dentro deste contexto, toda e qualquer informação deve ser correta, precisa, autêntica e estar disponível somente para a pessoa ou sistema adequado. Portanto, Segurança da Informação[1] se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa.

Uma política de segurança da informação[2] consiste num conjunto formal de regras que devem ser seguidas pelos usuários de informações de uma organização ou de uma pessoa.

A **Portofino** exerce atividades ligadas à Administração de Carteiras de Valores Mobiliários, função esta que significa a administração de recursos financeiros de terceiros (por ex., dinheiro da aposentadoria de uma pessoa, reservas para eventuais viagens ou infortúnios) e, dentre outras, de Serviços Pessoais e Patrimoniais, atividades estas ligadas a Administração ou Assessoria do Patrimônio Não Financeiro ou de Atividades Transacionais dos Clientes. O acesso por pessoa não autorizada a informações, bem como a perda, roubo ou a manipulação inadvertida destas podem gerar perdas significativas de imagem e danos financeiros, tanto para a **Portofino** quanto para seus Clientes, além das penalidades previstas na lei e em Normas regulamentares.

V – Princípios básicos da segurança da informação

São os princípios básicos da Segurança da Informação:

- **Confidencialidade**: limita o acesso à informação tão somente às pessoas ou instituições autorizadas pelo proprietário da informação;
- **Integridade**: garante que a informação tratada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição);
- **Disponibilidade**: garante que a informação esteja sempre disponível para o uso por aqueles usuários autorizados pelo proprietário da informação; e
- **Autenticidade**: propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um Processo.

O cumprimento desses 4 (quatro) princípios requer:

- Comprometimento da Alta Administração da empresa quanto ao tema;

[1] O conceito de Segurança da Informação está padronizado pela norma ISO/IEC 17799:2005, influenciada pelo padrão inglês BS7799.

[2] RFC 2196 (The Site Security Handbook).

- Metodologia de classificação das informações com a finalidade de que os colaboradores tenham ciência da criticidade de cada informação;
- Conscientização dos usuários quanto a importância do tema; e
- Implementação de um programa de segurança da Informação.

VI – Definições da LGPD

São as definições dos seguintes termos considerados especialmente relevantes para uma melhor compreensão desta Política:

• Controlador:	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
• Dado:	Códigos que constituem a matéria prima da informação, incluindo em seu conceito dado pessoal, dado pessoal sensível e outros;
• Dado pessoal:	Informação relacionada a pessoa física e/ou pessoa jurídica identificada ou identificável, nos termos da LGPD, incluso em conceito o dado pessoal sensível;
• Dado pessoal sensível:	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
• Operador:	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
• Titular:	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; e
• Tratamento:	Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

VII – Classificação e ciclo das informações

VII.1. Classificação das informações conforme a confidencialidade

Um dos critérios classificadores das informações tratadas pela **Portofino** é o da confidencialidade. Decorrem deste as seguintes abaixo.

VII.1.1. Informações de uso público

A informação deve ser classificada como pública quando ela puder ser divulgada a todos os colaboradores, terceirizados, Clientes, fornecedores e público em geral, sem que isso provoque impactos no negócio e desde que tenham se tornado públicos por intento do seu titular e que seja considerada a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. Apesar de uma informação pública não precisar de nenhum tipo de proteção quanto à questão do sigilo, é conveniente que usuário somente tenha acesso caso precise de tal informação para o desempenho de suas atividades.

Além disso, são consideradas informações de uso público todas as informações que por força de lei, norma ou Código de associação de classe, seja a **Portofino** obrigada a divulgar publicamente, desde que não conflite com nenhuma norma que hierarquicamente lhe seja superior.

VII.1.2. Informações de uso interno

A informação deve ser classificada como de uso interno quando não puder ser divulgada a terceiros ou ao público em geral, mas que não serão gerados grandes prejuízos na ocorrência de algum incidente de segurança de informação que a divulgue. Desta forma, são considerados exemplos de informações de uso interno: as convocações de reuniões e as regras de horários e expedientes.

VII.1.3. Informações restritas

A informação deve ser classificada como restrita quando sua exposição fora do ambiente da **Portofino** possa acarretar perdas financeiras, de imagem, de competitividade e de reputação.

Desta forma, são consideradas informações restritas para a **Portofino** todo tipo de informação escrita, verbal ou apresentada de modo tangível ou intangível acessadas pelo colaborador em virtude do desempenho de suas atividades combinado com a possibilidade de inclusão de:

- Dados pessoais de Clientes, Contrapartes comerciais, Fornecedores e Prestadores de Serviços[3];
- Relação de Clientes, Contrapartes comerciais, Fornecedores e Prestadores de Serviços;
- *Know-how*, técnicas, diagramas, modelos, e programas de computador;
- Informações técnicas, financeiras, mercadológicas ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de Clientes e Carteiras geridas pela **Portofino;**
- Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para Carteiras geridas pela **Portofino**;
- Estruturas e planos de ação;
- Qualquer informação relativa às Atividades da **Portofino,** seus Sócios ou seus Clientes;
- Informações e recursos disponíveis a projetos e trabalhos críticos para a continuidade do negócio da organização; e

[3] Inclusive conforme o que dispõem a L12527, art. 31, e a LGPD, art. 5.

- Toda e qualquer informação que por força de lei seja obrigatório o sigilo e confidencialidade.

VII.1.4. Informações confidenciais

A informação deve ser classificada como confidencial quando acessos não autorizados a ela, mesmo que por membros da **Portofino**, sejam capazes de trazer sérios danos ao negócio. Logo, a informação confidencial precisa ser protegida contra acessos internos e externos. São ainda mais importantes que as informações restritas e, por isso, devem receber um grau de proteção ainda mais elevado.

Só devem ter acesso a informações confidenciais pessoas que necessitem dessas informações para a realização de suas atividades, independentemente do cargo ocupado.

Logo, são consideradas informações confidenciais todas as que:

- Que envolvam dados pessoais sensíveis de Clientes, Contrapartes comerciais, Fornecedores e Prestadores de Serviço[4];
- Sejam de Áreas internas à **Portofino** e que, por força de lei, norma ou Ética, precisem ter segregação, por ex.: (i) gestão de recursos de terceiros, (ii) consultoria empresarial etc.;
- Não possam ser acessadas por determinados colaboradores e/ou Áreas em função de se trazer risco de geração de conflito de interesses na tomada de decisão;
- Identificação de transações ou de Clientes com indícios de LDFTC; e
- Sejam informações privilegiadas, tais como, as relacionadas a vida pessoal e profissional do Cliente que ainda não se tornaram públicas, senhas de Clientes etc.

VII.2. Ciclo das informações

O ciclo de vida da informação é composto por 4 (quatro) fases:

- **Manuseio**: ocorre quando a informação é recebida, criada e/ou manipulada (por ex., ler uma apresentação impressa, digitar informações em um *website*, utilizar senha de acesso a um sistema etc.);
- **Armazenamento**: a informação pode ser guardada em banco de dados, papel, "servidor" ou dispositivo de armazenamento (por ex., em "nuvem", *pen drive*, gaveta etc.);
- **Transporte**: momento em que a informação é distribuída e transportada via *e-mail*, telefone, reunião, veículo, entre outros;
- **Descarte**: evento que a informação é deletada, picotada, depositada em um lixo ou o equipamento é descartado.

VIII – Conscientização da importância da política de segurança da informação e da proteção de dados

[4] Inclusive conforme o que dispõem a L12527, art. 31, e a LGPD, art. 5.

VIII.1. Treinamento, compreensão e adesão da política

Para (i) garantir uma adequação aos princípios da segurança da informação, (ii) as diretrizes da **Portofino** e Normas legais de proteção de dados e (iii) os colaboradores entenderem a importância, é preciso assegurar que cada colaborador esteja em conformidade com as Normas descritas nesta Política e nas leis que regem o setor de atuação da **Portofino**. Além disso, a gestão da segurança da informação necessita do apoio e participação de todos os colaboradores no dia a dia de suas atividades.

Para tanto, é necessário que se adote os 4 (quatro) passos a seguir:

- Treinamento e compreensão desta Política;
- Assinatura do Termo de Ciência e Compromisso desta Política;
- Assinatura do Termo de Confidencialidade; e
- Reciclagem anual.

O cumprimento desses 4 (quatro) passos é de responsabilidade do Diretor de Compliance, o qual seguirá as seguintes regras:

- Adotar Processo de integração e treinamento inicial dos colaboradores, aos quais, antes do início de suas atividades, será apresentada a Política de Segurança da Informação e todos os documentos relacionados.
- Toda e qualquer dúvida, questionamento, sugestão ou pedido de esclarecimento relacionado a tais princípios e Normas, ou quaisquer outras, deverão ser respondidos em até 1 (um) dia útil para que os colaboradores possam compreendê-las e observá-las integralmente no desempenho das suas respectivas atividades; e
- Adotar programa periódico de reciclagem dos colaboradores com o objetivo de estarem atualizados em relação às mudanças nas regras de segurança da informação aplicáveis a **Portofino**.

VIII.2. Riscos de não cumprimento desta Política

Pretende-se com esta Política a mitigação de diversos riscos, sendo os seguintes alguns dos principais deles.

VIII.2.1. Ataque cibernético[5]

Existem diversas razões para que ataques cibernéticos sejam realizados. Os principais motivos identificados são:

- Obter ganho financeiro;
- Roubar, manipular ou adulterar informações;
- Obter vantagens competitivas e informações confidenciais de empresas concorrentes;
- Fraudar, sabotar ou expor a instituição invadida.

[5] Fonte: Guia ANBIMA de Cibersegurança, 2ª ed.

Os invasores podem utilizar vários métodos para os ataques cibernéticos. Destacam-se os mais comuns (vide "ANEXO V - Resumo Comparativo entre Códigos Maliciosos" desta Política para um resumo da forma de atuação dos invasores mais comuns):

- *Malware*: *softwares* desenvolvidos para corromper computadores e "redes":
    - Vírus: *software* que causa danos a máquina, "rede", outros *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*: *malware* malicioso que bloqueia o acesso a sistemas e bases de dados, ao solicitar 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 *website* 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 e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas de um ente; no caso dos *botnets*, o ataque vem de muitos computadores infectados utilizados para criar e mandar *spam* ou vírus, ou inundar uma "rede" com mensagens resultando na negação de serviços; e
- APT: ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

VIII.2.2. Perda financeira

O não cumprimento dos princípios de segurança da informação (confidencialidade, integridade, disponibilidade e autenticidade) pode gerar perdas financeiras aos Clientes, multas a **Portofino** por descumprimento a Normas e leis e até mesmo perda da autorização do exercício de determinadas atividades.

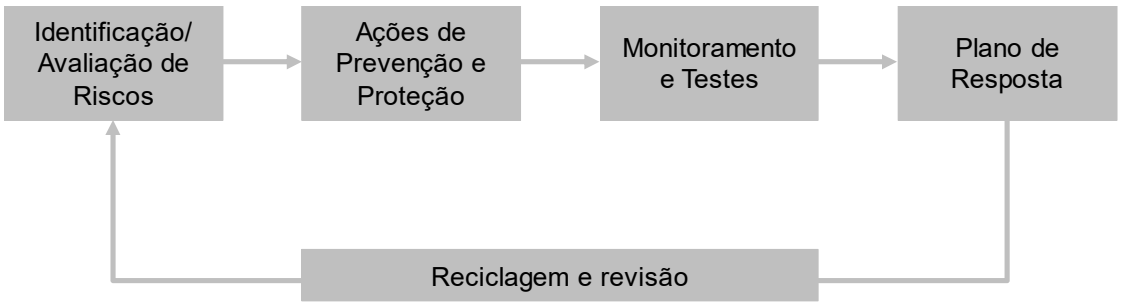
VIII.2.3. Risco de imagem e risco operacional

A perda de integridade, a não disponibilidade e a falta de autenticidade da informação podem gerar tomada de decisão na execução de atividades (por ex., investimento etc.) equivocada, o retardo

nesta tomada, a perda do prazo de cumprimento de obrigações e de negociação de um ativo e, consequentemente, uma exposição negativa perante os "*stakeholders*".

IX – Programa de segurança da informação e de proteção de dados

A **Portofino** adota um programa de segurança da Informação que engloba as seguintes 5 (cinco) macro atividades:



IX.1. Identificação / avaliação de riscos

Tem por **objetivo** identificar os riscos internos e externos quanto aos ativos e Processos que precisam de proteção.

Os esforços são compatíveis com as características e o tamanho da instituição, e os recursos de defesa e as respostas proporcionais aos riscos identificados. A Avaliação leva em conta o ambiente da Instituição, seus Objetivos, seus *Stakeholders* e suas Atividades[6].

A **forma de atuação** consiste em:

1. Identificar todos os Processos e ativos (equipamentos, sistemas e dados) relevantes;
2. Identificar e avaliar o tratamento de dados, as vulnerabilidades e os riscos de segurança da informação; e
3. Estimar os impactos financeiros, operacionais e de reputação.

Todo este ciclo do Programa de Segurança da Informação é documentado na "Matriz de Processos e Ativos Críticos para fins de PCN".

IX.2. Ações de prevenção e proteção

Tem por **objetivo** estabelecer e implementar medidas para mitigar e minimizar a concretização dos riscos identificados no item "IX.1. Identificação / Avaliação de Ativos" desta Política.

A **forma de atuação** consiste em:

[6] Guia ANBIMA de Cibersegurança, 2ª ed.

1. Implementar regras para tratamento de dados pessoais, e manuseio, armazenamento, transporte e descarte das demais informações (vide "Anexo I – Regras de Manuseio, Armazenamento, Transporte e Descarte das Informações" desta Política);

2. Definir e implementar ações de proteção, prevenção e remediação das vulnerabilidades e riscos identificados na etapa acima (vide "Matriz de Processos e Ativos Críticos para fins de PCN" da **Portofino** e os Anexos desta Política);

3. Na contratação de serviços de Terceiros relevantes, realizar a diligência de modo a verificar se estes possuem padrões de Segurança da Informação de acordo com as informações que vierem a manusear, armazenar, transportar ou descartar (vide "Política de Contratação de Terceiros" da **Portofino**); e

4. Treinar e conscientizar os colaboradores quanto a importância da Segurança da Informação e de Proteção de Dados (vide Item "VIII. Conscientização da Importância da Política de Segurança da Informação e de Proteção e Privacidade de Dados Pessoais" e Anexos desta Política).

IX.3. Monitoramento e testes

Tem por **objetivo** detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

A **forma de atuação** consiste em:

1. Monitorar a implementação e a execução das ações definidas no item "IX.2. Ações de Prevenção e Proteção" desta Política;

2. Monitorar, na periodicidade de acordo com o risco que representa, os relatórios de supervisão, *logs* e trilhas de auditoria;

3. Monitorar diariamente as rotinas de *backup*;

4. Monitorar quais equipamentos possuem acesso remoto aos dados e sistemas da **Portofino**;

5. Realizar anualmente testes de contingência e de restauração de dados;

6. Realizar supervisão baseada em risco dos Prestadores de Serviços e Fornecedores que possuem informações da **Portofino** (vide "Política de Contratação de Terceiros" da **Portofino**).

Para maiores informações, vide o "Anexo II - Monitoramento e Controle de Manuseio, Armazenamento, Transporte e Descarte de Informações" desta Política.

IX.4. Plano de resposta

Tem por **objetivo** um Plano de Resposta, Tratamento e Recuperação de Incidentes, incluindo um Plano de Comunicação interna e externa, caso necessário.

A **forma de atuação** consiste em:

1. Elaborar um Plano de Continuidade de Negócios, atentando para a segurança e controles da contingência (vide "Plano de Continuidade de Negócios" da **Portofino**);

2. Elaborar plano de resposta de acordo com a severidade do incidente quando da identificação da inobservância de um ou mais dos princípios de Segurança da Informação (confidencialidade, integridade, disponibilidade e autenticidade) e de Proteção de Dados (vide "Anexo III – Gestão de Incidentes de Segurança da Informação e de Proteção de Dados" desta Política e a "Política de Privacidade" da **Portofino**); e

3. Arquivar documentos relacionados ao Programa de Segurança da Informação por ao menos 5 (cinco) anos.

IX.5. Reciclagem e revisão

Tem por **objetivo** manter o Programa de Segurança da Informação e de Proteção de Dados continuamente atualizado, identificando novos riscos, ativos e Processos e reavaliando os riscos residuais.

A **forma de atuação** consiste em:

1. Instituir Comitê de Segurança da Informação (vide Item "X. Governança" desta Política);

2. Elaborar Relatório trimestral de Segurança da Informação; e

3. Revisar o Programa anualmente ou sempre que o Comitê de Segurança da Informação achar necessário.

X – Governança

X.1. Comitê de segurança da informação

Responsabilidades	• Aprovar alterações desta Política, da "Política de Privacidade", da "Matriz de Processos e Ativos Críticos para fins de PCN" e da Infraestrutura de Segurança da Informação, todos da **Portofino**; • Manter-se atualizado quanto a novas vulnerabilidades; • Atuar em conjunto com o Diretor responsável por esta Política para tornar efetivo o Programa de Segurança da Informação e de Proteção de Dados; • Rever tratamento de dados, classificação das informações e direito de acesso a estas por cada Área; • Verificar o cumprimento a esta Política com base nos Relatórios disponibilizados; • Gerenciar incidentes de Segurança da Informação e de Proteção de Dados.
Composição	• Responsável: Diretor de Compliance;

	• Demais membros: Diretoria da **Portofino**, responsável pela Tecnologia da Informação da **Portofino** e Assistente direto, Assistente de Compliance e Assistente de Gestão de Riscos.
Periodicidade	• Trimestral para acompanhamento dos Processos e controles de segurança da informação, ou mediante convocação do Diretor responsável por esta Política; e • Anual para a revisão desta Política.

X.2. Responsabilidades

Área	Responsabilidades
• Colaboradores:	• Seguirem todas as regras definidas nesta Política, seus Anexos e "Matriz de Processos e Ativos Críticos para fins de PCN".
• Diretoria de Compliance:	• Coordenar a implementação do Programa de Segurança da Informação; e • Atualizar esta Política.
• Área de Tecnologia da Informação:	• Monitorar a infraestrutura, dos equipamentos / dispositivos e demais itens para o devido cumprimento das diretrizes estabelecidas nesta Política; e • Elaborar os Relatórios e monitorar os *logs* e trilhas de auditoria.
• Encarregado da LGPD:	• Atuar como canal de comunicação entre o Controlador, os Titulares dos dados e a ANPD, aceitando reclamações, prestando esclarecimentos e adotando providências; • Atualizar a "Política de Privacidade" da **Portofino**; • Garantir que seu contato esteja disponível no *website* da **Portofino**; • Orientar os colaboradores da **Portofino** a respeito das práticas a serem tomadas em relação à proteção de Dados Pessoais; • Comunicar incidentes de proteção de Dados Pessoais à ANPD e ao titular dos mesmos; • Elaborar, sob demanda da ANPD, Relatório de Impacto à Proteção de Dados Pessoais, referente a suas operações de tratamento de Dados e/ou quando o tratamento tiver como fundamento seu interesse legítimo; e • Executar as demais atribuições determinadas pelo controlador ou estabelecidas em Normas complementares.

XI – Disposições gerais

XI.1. Documentação

Cada colaborador, no âmbito de sua atuação conforme esta Política, deve manter registrado e arquivado pelo período mínimo indicado pela Área de Compliance as informações e documentos objeto de seu trabalho.

Tal prazo não será menor do que o de 5 (cinco) anos contados da ocorrência do evento, podendo ser estendido pela mesma Área indefinidamente na hipótese de existência de investigação comunicada formalmente à **Portofino** por Autoridade ou afim, ou, ainda, por terceiro interessado.

XI.2. Infrações

O descumprimento das Normas previstas na presente Política poderá provocar a abertura de Processo Interno de Averiguação de Irregularidades e sujeitar o responsável envolvido a medidas disciplinares, incluindo, mas não se limitando, às penalidades previstas no "Regulamento Interno" da **Portofino**.

XI.3. Situações não previstas nesta política

Todas as situações não previstas nesta Política e identificadas por qualquer colaborador, Prestador de Serviço, Cotista de FIs eventualmente por ela geridos, Órgão Fiscalizador ou Regulador da **Portofino** devem ser levadas tempestivamente ao conhecimento do Diretor de Compliance desta. Conforme o caso, este deve atuar de modo com que se:

- Avalie e documente a situação identificada;
- Convoque extraordinariamente o Comitê de Segurança da Informação;
- Adeque esta Política e a publique apropriadamente; e
- Instrua as Áreas envolvidas quanto aos novos Procedimentos.

XI.4. Treinamento e disseminação do conteúdo

Todos os colaboradores da **Portofino** devem receber Treinamento sobre esta Política e a Legislação pertinente, inclusive tendo-se por finalidade a de estabelecimento de um canal informativo sobre como o tema deve ser tratado por todos na Empresa.

Tais Treinamentos devem ser realizados em relação a cada colaborador na ocorrência de cada um dos eventos a seguir: (a) início da relação com a **Portofino**; (b) transferência para funções críticas do Negócio, principalmente daqueles que pertençam à equipe de Compliance e Tecnologia da Informação, devendo serem instruídos acerca das suas respectivas responsabilidades conforme a Política; e (c) anualmente, a título de Reciclagem.

Adicionalmente, todos os colaboradores devem receber uma cópia da presente Política e cada nova alteração, ao que devem atestar a ciência e o entendimento das disposições nelas constantes, bem como o compromisso de cumpri-los.

Em caso de dúvidas, a Área responsável pelo presente deve ser imediatamente contatada.

Os registros de tal termo, bem como do material utilizado e o controle efetivo de participação dos colaboradores nos Treinamentos devem ser mantidos pela Área de Compliance nos termos do Item "XI.1. Documentação" desta Política.

XI.5. Ciência dos colaboradores quanto ao monitoramento de atividades

Os colaboradores da Portofino ficam desde já cientes de que, com o intuito de identificar casos suspeitos ou efetivamente em desconformidade com a presente Política e demais Documentos e Normas aplicáveis, a Portofino poderá monitorar quaisquer Atividades por eles desenvolvidas.

XI.6. Atualização da política

A atualização desta Política deve ocorrer anualmente ou conforme novas Regulamentações assim demandarem, assim como pelo uso de novas tecnologias e novos serviços a serem prestados. Tais alterações serão válidas, eficazes e vinculantes a partir de sua publicação.

Adicionalmente, a **Portofino** poderá publicar Normas adicionais, complementares e/ou de atualização, devendo ser conferida a necessária divulgação aos colaboradores.

Ademais, a Área de Compliance deve atualizar este com base na Revisão do Comitê de Segurança da Informação.

XI.7. Vigência

As Normas dispostas no presente documento substituem as anteriormente publicadas e com aquelas conflitem, entrando em vigor na data estabelecida em sua capa.

Anexo I – Regras de manuseio, armazenamento, transporte e descarte das informações

A.I.1. Política de e-mails

- É proibida a abertura de anexos com as extensões dos tipos ".bat", ".exe", ".src", ".lnk" e ".com" se não tiver certeza de que (i) solicitou o *e-mail*, (ii) o remetente é confiável e (iii) este tenha confirmado oralmente o seu envio;
- É exigida a desconfiança por parte dos colaboradores de todos os *e-mails* com assuntos com termos estranhos. Exemplos: "ILOVEYOU", "Branca de Neve Pornô", "Veja as fotos da (...)", "ganhe dinheiro sem sair de casa", "sua senha do banco será revogada", "seu nome será negativado" etc.
- É proibido o acesso a conta de *e-mail* pessoal pelos computadores, celulares, *tablets* ou qualquer outro equipamento da **Portofino** ou utilizando a "rede" / *internet* desta;
- O *e-mail* da **Portofino** é de uso estritamente profissional, não devendo ser utilizado para fins pessoais;
- Os colaboradores não poderão usar intencionalmente o *e-mail* da **Portofino** para distribuir "correntes", brincadeiras, enviar material ofensivo, inadequado ou que promova qualquer tipo de discriminação racial;
- Se o colaborador receber um *e-mail* para distribuição a outras pessoas, como uma corrente, não poderá enviá-lo;
- Se tiver qualquer suspeita de que recebeu um vírus, o colaborador deverá entrar em contato com a Área de Tecnologia da Informação imediatamente;
- Qualquer acesso ao *e-mail* em nova estação de trabalho ou dispositivo deverá ser autorizado pela Área de Tecnologia da Informação da **Portofino.**

A.I.1.1. Aviso em e-mail

Todos os *e-mails* da **Portofino** devem conter *disclaimer* nos seguintes termos:

Esta mensagem pode conter informação confidencial e/ou privilegiada. Se você não for o destinatário ou a pessoa autorizada a receber esta mensagem, não pode usar, copiar ou divulgar as informações nela contidas ou tomar qualquer ação baseada nessas informações. Se você recebeu esta mensagem por engano, por favor avise imediatamente o remetente, respondendo o *e-mail* e em seguida apague-o.	This message may contain confidential and/or privileged information. If you are not the addressee or authorized to receive this for the addressee, you must not use, copy, disclose or take any action based on this message or any information herein. If you have received this message in error, please advise the sender immediately by reply e-mail and delete this message.

A.I.2. Política de senhas

- Os colaboradores devem utilizar sempre senhas alfanuméricas (letras e números) com diferentes caixas (maiúscula e minúscula) e caracteres especiais;
- Os colaboradores devem sempre manter as suas senhas seguras e não as revelar a ninguém, como tampouco deixá-las anotadas;
- Tudo que for executado com suas senhas será de inteira responsabilidade do colaborador, excetuando-se casos de comprovadas vulnerabilidades da infraestrutura de segurança da informação;
- Não devem ser utilizadas senhas fáceis de serem descobertas, tais como nome da esposa, dos filhos, datas comemorativas pessoais etc.; e
- É recomendável que as senhas de acesso às estações de trabalho sejam atualizadas a cada 90 (noventa) dias.

A.I.3. Política de internet

- O acesso ao sinal de *internet* fornecido pela **Portofino** é de uso estritamente profissional, não devendo ser utilizada para fins pessoais. Os colaboradores não devem entrar em *websites* com conteúdo ofensivo, inadequado ou que promova qualquer tipo de discriminação racial, social ou moral;
- É proibido o uso de ferramentas "P2P" (por ex., Kazaa, Morpheus, Bit Torrent etc.);
- É proibido o uso de *instant messengers* não homologados ou autorizados pela Área de Tecnologia da Informação, excetuando o Whatsapp (vide item "A.I.7. Política de Uso de Aplicativos de Mensagens Instantâneas" desta Política); e
- A Área de Tecnologia da Informação analisa mensalmente os *websites* que os colaboradores navegam de forma a verificar se estes estão utilizando a *internet* somente para fins profissionais.

A.I.4. Política de uso da estação de trabalho

Cada estação de trabalho tem Códigos internos que permitem que ela seja identificada na "rede", e cada indivíduo possui sua própria estação de trabalho e *login* de acesso à "rede" da **Portofino**. Isso significa que tudo o que venha a ser executado de sua estação acarretará responsabilidade ao colaborador. Por isso, devem os colaboradores, sempre que saírem de sua estação de trabalho, ter certeza de que efetuou o *logoff* ou bloqueou o acesso ao equipamento.

A.I.4.1. Download e instalação de software

Todo *software* somente poderá ser instalado mediante autorização da Área de Tecnologia da Informação.

É proibido o *download* de aplicativos e de *software* não autorizado pela Área de Tecnologia da Informação em razão da possibilidade de abertura de brechas no *firewall* da **Portofino**.

Recomenda-se a consulta pelos colaboradores junto à Área de Tecnologia da Informação da lista de *softwares* autorizados para saber se pode ou não ser instalado.

A.I.4.2. Proteção da "rede" e antivírus

O "servidor", os computadores e demais dispositivos da **Portofino** utilizam antivírus cuja atualização é realizada todos os dias de forma automática.

O antivírus está configurado de forma a verificar ameaças da *internet*, de *e-mails* e de toda e qualquer origem de fonte de informação externa à **Portofino**.

A renovação da licença do antivírus também deve ser realizada automaticamente pela Área de Tecnologia da Informação.

A.I.4.3. Bloqueio da estação de trabalho

Ao se ausentar de sua mesa, o funcionário deve bloquear a sua estação de trabalho, garantindo assim que o acesso às informações ali armazenadas só possa ser realizado através do desbloqueio com senha.

A.I.5. Política social

Os colaboradores não devem:

- Revelar a terceiros que não tenham autorização sobre o assunto ou em locais públicos informações sobre esta Política ou sobre qualquer item a ela relacionado;
- Revelar a senha para ninguém;
- Digitar as senhas em máquinas que não sejam da **Portofino**;
- Digitar as senhas em uma estação de trabalho que não seja a sua;
- Digitar as senhas quando estiver habilitada a opção de sua memorização;
- Revelar informações da **Portofino** para pessoa não identificada ou desconhecida, mesmo que ela se apresente como sendo colaborador de ente com o qual a **Portofino** tenha relacionamento; e
- Conversar sobre assunto profissional em elevador, táxi, bar, restaurante e outros recintos públicos.

Devem os colaboradores, no entanto, relatar à Área de Compliance pedidos internos e externos que venham a conflitar com qualquer Item desta Política.

A.I.6. Política de uso de celulares (voz)

A utilização de celulares com os seguintes intuitos apresenta algumas fragilidades quanto a formalização e documentação dos atos exigidos pela regulamentação em vigor:

- Executar compra e venda ou outras movimentações de ativos pertencentes a Carteira de Investimentos de Clientes;
- Tratar de propostas comerciais com Clientes; e
- Manipular informações confidenciais, dentre outras.

Por isto, toda e qualquer ligação e/ou troca de mensagens com conteúdo relevante via aplicativos de mensagens instantâneas com Clientes, fornecedores e demais pessoas referentes a serviços prestados pela **Portofino** devem ser transcritas para um *e-mail* de forma a se possibilitar a efetiva documentação e arquivamento.

A.I.7. Política de uso de aplicativos de mensagens instantâneas

Aplicativos de mensagens instantâneas (por ex., WhatsApp, etc.) e de aplicativos de videoconferência (por ex., Zoom, Google Meets, Microsoft Teams etc.) são ferramentas que permitem o envio e o recebimento de mensagens em tempo real, sendo extremamente populares nos dias de hoje.

Em função das limitações que estes aplicativos possuem, toda e qualquer comunicação com o Cliente, Contrapartes de transações relevantes de Clientes, de Fornecedores e de Prestadores de Serviço relevantes deve ser feita preferencialmente via *e-mail* corporativo da **Portofino**.

Caso não seja possível, em razão do hábito dos Clientes, deve-se sintetizar a conversa com o Cliente em um *e-mail* para formalizar as instruções dadas por este, bem como as decisões tomadas.

A.I.8. Política de segregação de atividades

A Administração de Carteiras de Valores Mobiliários deve ser segregada das demais atividades exercidas pela **Portofino**, por meio da adoção dos seguintes Procedimentos[7]:

A.I.8.1. Segregação física

A Resolução CVM 21, em seu art. 27, inciso I, exige a segregação física de instalações entre as Áreas responsáveis pela Administração de Carteiras de Valores Mobiliários e as Áreas responsáveis pela Intermediação e Distribuição de Valores Mobiliários.

Como a **Portofino** não atua com a Intermediação e Distribuição de Valores Mobiliários, não é necessário realizar a segregação física.

A.I.8.2. Chinese Wall

Com a finalidade de se evitar o uso e o acesso a informações privilegiadas, a **Portofino** utiliza-se do conceito *Chinese Wall*, o qual segrega as informações de colaboradores envoltos em atividades de Gestão das relacionadas às demais atividades.

Este muro de informações é controlado e mantido pelo Diretor de Compliance que tem acesso a informações de ambos os lados e se incumbe de manter a integridade da segregação, através da supervisão das atividades da **Portofino** e de seus colaboradores.

A comunicação entre as Áreas separadas pelo *Chinese Wall* deve ser feita como se fossem de empresas distintas, seguindo as Normas desta Política.

A.I.8.3. Criação e manutenção de usuários

Os acessos internos e externos aos serviços de "rede", "servidores", armários, sistemas e *e-mail* da **Portofino** são liberados de acordo com a função que o colaborador exerce na Empresa e de acordo

[7] Inclusive conforme o que dispõe a Resol. CVM 21, art. 27.

com a sua necessidade. As Áreas de Tecnologia da Informação e de Compliance são responsáveis por definir os acessos de todos os colaboradores.

Quando da troca de função dentro da empresa, as Áreas de Tecnologia da Informação e de Compliance devem obrigatoriamente serem avisadas de imediato e os acessos revistos em virtude do exercício da nova função.

Quando do desligamento de colaboradores, os seus acessos à "rede", "servidores", armários, sistemas e *e-mail* são revogados a partir do momento em que tal evento for informado à Área de Tecnologia da Informação e de Compliance. O líder da equipe até então integrada pelo colaborador é o responsável pela notificação.

A.I.9. Política de manuseio, armazenamento, transporte e descarte de arquivos

A **Portofino** deve manter digitalmente, pelo prazo mínimo de 5 (cinco) anos, ou por prazo superior por determinação expressa da CVM, RFB, demais órgãos reguladores e pela Área de Compliance, todos os documentos e informações, bem como toda a correspondência, interna e externa, todos os papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções[8].

É de responsabilidade de cada colaborador da **Portofino** gravar tempestivamente e manter organizado nos "servidores", armários e seus sistemas, todo e qualquer arquivo, documento, relatório, pesquisa, banco de dados, sistema, informação e planilha objeto de seu trabalho.

Os armários de arquivos de documentos físicos devem ser trancados por chave.

A chave dos armários físicos de cada sítio deve permanecer sob a responsabilidade de colaborador específico que nele tenha a sua estação de trabalho e uma cópia no cofre, localizado no respectivo sítio. O colaborador que precise acessar o armário deverá solicitar o acesso da chave ao colaborador responsável por ela.

A.I.9.1. Realização de cópias de segurança

Cópias de segurança dos dados do "servidor" e da nuvem devem ocorrer diariamente, devendo a Área de Tecnologia da Informação verificar nesta mesma frequência se a cópia está sendo executada.

A.I.9.2. Política de distribuição e transporte de informações

É terminantemente proibido aos colaboradores fazerem cópias (físicas ou eletrônicas) de arquivos contendo informações de propriedade da **Portofino**, do cliente e de terceiros relacionados a **Portofino**, e circular em ambientes externos à empresa ou dar acesso a colaboradores ou terceiros não autorizados especificamente pela Área de Compliance.

Além disto, o acesso ao dispositivo para o respectivo acesso eletrônico deve se dar com a autenticação do usuário com a senha correspondente devido à criptografia dos equipamentos.

Qualquer situação que acarrete um acesso de forma diferente do previsto, levará à inutilização do equipamento para acesso eletrônico e dos dados nele constantes (por ex., em caso de furto ou roubo de equipamento).

[8] Inclusive conforme o que dispõe a Resol.CVM 21, art. 34.

No que tange a distribuição e transporte dos documentos em formato físico, exige-se que o colaborador obtenha do receptor protocolo que ateste o recebimento.

A.I.9.2.1. Acesso remoto à "rede"

Por definição, acesso remoto é uma tecnologia que permite que um dispositivo (por ex., computador, *tablet*, celular etc.) não conectado fisicamente à "rede" de uma empresa consiga acessá-la.

Em função das regras legais e das informações confidenciais que a **Portofino** manuseia, bem como o risco do transporte dessa informação para fora da companhia, os equipamentos que puderem acessar informações, tais como, mas não se limitando àqueles dispostos em arquivos no servidor e em *e-mails* da **Portofino** fora do escritório devem todos atenderem aos requisitos de segurança estabelecidos pela Área de TI. Esta Área deve catalogar todos os equipamentos que possuem este acesso e as configurações de segurança instalados/utilizados nestes.

A.I.9.3. "Firewall"

Somente a Área de Tecnologia da Informação está habilitada para proceder com as seguintes ações em relação ao *firewall*:

- **Alteração da configuração**;
- **Monitoramento**; e
- **Atualização**.

A.I.9.4. Descarte de ativos

Toda informação que precise ser descartada deve seguir os seguintes Procedimentos:

• Arquivos magnéticos:	devem ser apagados definitivamente (remover do disco e deixar o espaço vazio);
• Arquivos em papel:	devem ser triturados; e
• Login de acesso:	devem ter sua senha e *login* revogados e depois excluídos.

A.I.10. Avisos importantes em apresentações

Todas as páginas de apresentação a Clientes, Contrapartes comerciais, Fornecedores e Prestadores de Serviços que possuam informações classificadas como confidenciais devem conter aviso de que o material é confidencial e de propriedade da **Portofino**.

Anexo II – Monitoramento e controle de manuseio, armazenamento, transporte e descarte de informações e dados

A.II.1. Política de monitoramento de atividades

A.II.1.1. Monitoramento dos meios de comunicação

Para assegurar o fiel cumprimento das regras internas, como também da Legislação vigente, a Portofino se reserva no direito de rastrear, monitorar, gravar e inspecionar todo e qualquer tráfego de voz, imagem e texto realizado através de contato telefônico, internet, intranet, sistema de mensagem instantânea, fax, correio físico e eletrônico (e-mail), bem como os arquivos armazenados ou criados pelos recursos da informática pertencentes à Portofino ou utilizados em nome dela.

A.II.1.2. Monitoramento da "rede"

A Área de Tecnologia da Informação deve:

- Providenciar o registro de trilhas de auditoria, assim como as exceções e outros eventos de segurança relevantes, por um período determinado pela própria; e
- Monitorar as trilhas de auditoria e os acessos as pastas, arquivos e "rede" de forma a verificar qualquer violação das regras acima.

A.II.1.3. Monitoramento dos sistemas

Para os sistemas em que haja a funcionalidade, deve a Área de Tecnologia da Informação monitorar os acessos a estes, incluindo erro de senhas e atividades desempenhadas.

A Área também deve proteger os recursos computacionais contra adulteração e devem manter registros que permitam a realização de auditoria e inspeções[9].

A.II.1.4. Monitoramento de acesso à "rede", "servidores" e armários

O monitoramento de acesso à "rede" consiste em:

- Identificar o usuário que a acessa; e
- Verificar se o usuário que acessou determinada informação possui a respectiva permissão.

No caso de acesso aos armários de arquivo de documentos físicos, a Área de Compliance deve monitorar periodicamente se os armários nos quais estejam armazenados os arquivos físicos estão devidamente trancados com chave.

[9] Inclusive conforme o que dispõe a Resol.CVM 21, art. 4, §8º.

Anexo III – Gestão de incidentes de segurança da informação e de proteção de dados

Qualquer política de segurança da informação e de dados e controles propostos por um programa adequado muito embora devam visar a mitigação dos riscos relacionados à segurança, não garantem a proteção total dos ativos.

Em menor ou maior escala, as vulnerabilidades residuais existem e podem tornar ineficaz a proteção a informação e dados. Além disso, é inevitável que novas instâncias de ameaças anteriormente não identificadas ocorram.

Portanto, é preciso manter um Processo interno de gestão de incidentes com foco específico em segurança da informação e proteção de dados. Segundo a CERT.br, um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança de sistemas de computação ou de "redes" de computadores.

Exemplos de incidentes de segurança da informação incluem, mas não estão limitados a:

- Divulgação não autorizada ou acidental de informações sigilosas ou confidenciais, por ex., o *e-mail* contendo informações confidenciais ou sensíveis enviadas para destinatários incorretos etc.;
- Roubo ou perda de informações confidenciais, por ex., cópia impressa de informações confidenciais ou reservadas roubadas ou esquecidas em lugar de livre circulação de pessoas etc.;
- Modificação não autorizada de informações confidenciais ou reservadas;
- Roubo ou perda de equipamento que possua informações confidenciais ou acesso a elas, por ex., *tablet*, celulares ou computadores contendo informações confidenciais com acesso a "rede" etc.;
- Desconfiguração de portal eletrônico;
- Propagação de um vírus ou *worm* por meio da lista de contatos de e-mails;
- Recebimento de *spam*;
- Lentidão repentina de equipamentos;
- Recebimento de notificações estranhas;
- Enfrentamento de *pop-ups* excessivos durante a navegação;
- Aparição em equipamentos de arquivos não vistos anteriormente;
- Perda parcial ou completa de arquivos ou do disco rígido;
- Modificação sem solicitação de página eletrônica;
- Apresentação pelo navegador de nova barra de ferramentas sem que tenha sido solicitado;
- Envio de *e-mails* estranhos de forma automática pela conta de algum colaborador; e

- Antivírus que não realiza atualizações ou fornece mensagens de erro obscuras.

O Processo de Gestão de Incidentes mostra grande variação em sua implementação, dependendo em parte considerável do tamanho da empresa, da complexidade das atividades exercidas pela empresa e da regulamentação a que a empresa é obrigada a seguir, dentre outros fatores.

A.III.1. Política de gestão de incidentes de segurança

A Gestão de Incidentes de Segurança da Informação compreende as seguintes etapas:

1. Detecção e Análise;
2. Contenção, Erradicação e Recuperação; e
3. Atividades Pós-Incidente, incluindo Notificações, quando aplicável.

Em função (i) da complexidade do assunto, (ii) do mapeamento das ações a serem tomadas no caso de um incidente, e (iii) da evolução constante de novas ameaças, caso haja alguma suspeita de incidente, deve o colaborador relatá-la a um dos membros do Comitê de Segurança da Informação.

Todos os Procedimentos das atividades a serem desempenhadas em caso da ocorrência de incidentes devem estar detalhados na "Matriz de Processos e Ativos Críticos para fins de PCN" da **Portofino**.

A.III.2. Incidentes de proteção de dados pessoais

A **Portofino** deverá comunicar à ANPD e ao Titular dos dados pessoais a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

A comunicação deverá ser feita em até 3 (três) dias úteis da ocorrência[10], e deverá mencionar, no mínimo:

- A descrição da natureza dos dados pessoais afetados;
- As informações sobre os titulares envolvidos;
- A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- Os riscos relacionados ao incidente;
- Os motivos da demora, no caso de a comunicação não ter sido imediata; e
- As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

A ANPD verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao Controlador a adoção de providências, tais como:

- Ampla divulgação do fato em meios de comunicação; e
- Medidas para reverter ou mitigar os efeitos do incidente.

[10] A vigorar conforme decisão própria enquanto não disposto outro prazo pela ANPD, inclusive conforme dispõe a LGPD, art. 48, § 1º.

No juízo de gravidade do incidente, após Procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios, serão avaliadas o(a):

- Gravidade e a natureza das infrações e dos direitos pessoais afetados;
- Boa-fé do infrator;
- Vantagem auferida ou pretendida pelo infrator;
- Condição econômica do infrator;
- Reincidência;
- Grau do dano;
- Cooperação do infrator;
- Adoção reiterada e demonstrada de mecanismos e Procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com as medidas para reverter ou mitigar os efeitos do incidente;
- Adoção de política de boas práticas e governança;
- Pronta adoção de medidas corretivas; e
- Proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Para mais informações, vide a “Política de Privacidade” da **Portofino**.

Anexo IV – Procedimentos relativos a dados pessoais

A.IV.1. Direitos de clientes, colaboradores e terceiros relativos ao tratamento de dados pessoais

Os Titulares de Dados Pessoais possuem diversos direitos sobre eles quando tratados pela **Portofino**, dentre eles os seguintes:

• **Informação**:	direito de receber informações sobre a forma, os Agentes e outras questões relativas ao Tratamento de seus Dados Pessoais;
• **Retificação, complementação e atualização**:	direito de que os Dados Pessoais tratados pela **Portofino** sejam corrigidos, complementados ou atualizados na base de dados da **Portofino**, caso nesta estejam incorretos ou desatualizados;
• **Eliminação ("direito de ser esquecido")**:	direito de deleção de Dados Pessoais da base de dados da **Portofino**;
• **Portabilidade**:	direito de exigir a transferência de Dados Pessoais de maneira consolidada e na situação em que se encontrem para um novo prestador de serviço;
• **Personalização**:	direito de solicitar a personalização do Tratamento pela **Portofino** de Dados Pessoais do Titular, a ser acordado entre as partes;
• **Oposição**:	direito a se opor ao Tratamento pela **Portofino** de Dados Pessoais do Titular em determinadas circunstâncias e sob determinadas formas;
• **Revisão de decisões tomadas unicamente com base no Tratamento automatizado**:	direito de exigir (i) a revisão de decisões tomadas unicamente com base em Tratamento automatizado de Dados Pessoais que afetem os interesses dos Titulares, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito e os aspectos de sua personalidade; e (ii) informações claras e adequadas a respeito dos critérios e dos Procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial;
• **Anonimização**:	direito de exigir a utilização de meios técnicos razoáveis e disponíveis no momento do Tratamento, por meio dos quais um Dado perde a possibilidade de associação, direta ou indireta, ao Titular;
• **Consentimento**:	direito de que (i) antes do Tratamento de Dado Pessoal em determinados casos, seja obtido junto ao Titular a manifestação livre, informada e inequívoca pela qual concorda com o Tratamento para uma finalidade determinada, além de ser informado sobre a possibilidade de não fornecer consentimento para o tratamento dos seus dados e sobre as consequências dessa recusa; (ii) bem como de revogar o consentimento a qualquer tempo;

• **Reprodução**:	direito de obter cópia integral de seus dados pessoais em formato que permita a sua utilização subsequente;
• **Bloqueio**:	direito de que seja suspensa temporariamente determinada Operação de Tratamento de Dados Pessoais do Titular, mediante armazenamento pelo Controlador;
• **Transferência internacional**:	direito de que Dados Pessoais do Titular sejam tratados no exterior do Brasil, inclusive por terceiro, ou por organismo internacional do qual o país seja membro; e
• **Divulgação**:	direito de que Dados Pessoais do Titular sejam transferidos, disseminados, comunicados, transmitidos ou distribuídos para terceiros.

A.IV.2. Procedimentos relevantes passíveis de solicitação pela ANPD

Relatório de Impacto à Proteção de Dados:

Deverá conter, no mínimo:

- Descrição dos tipos de dados coletados;
- Metodologia utilizada para a coleta e para a garantia da segurança das informações;
- Análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados; e
- Descrição dos Processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais.

Para mais informações, vide a “Política de Privacidade” da **Portofino**.

Anexo V – Resumo comparativo entre Códigos maliciosos[11]

Códigos Maliciosos							
	Vírus	*Worm*	*Bot*	*Trojan*	*Spyware*	*Backdoor*	*Rootkit*
Como é obtido:							
Recebido automaticamente pela "rede"		✔	✔				
Recebido por *e-mail*	✔	✔	✔	✔	✔		
Baixado de *websites* na *internet*	✔	✔	✔	✔	✔		
Compartilhamento de arquivos	✔	✔	✔	✔	✔		
Uso de mídias removíveis infectadas	✔	✔	✔	✔	✔		
"Redes" sociais	✔	✔	✔	✔	✔		
Mensagens instantâneas	✔	✔	✔	✔	✔		
Inserido por um invasor		✔	✔	✔	✔	✔	✔
Ação de outro Código malicioso		✔	✔	✔	✔	✔	✔
Como ocorre a instalação:							
Execução de um arquivo infectado	✔						
Execução explícita do Código malicioso		✔	✔	✔	✔		
Via execução de outro Código malicioso						✔	✔
Exploração de vulnerabilidades		✔	✔			✔	✔
Como se propaga:							
Insere cópia de si próprio em arquivos	✔						
Envia cópia de si próprio automaticamente pela "rede"		✔	✔				
Envia cópia de si próprio automaticamente por *e-mail*		✔	✔				
Não se propaga				✔	✔	✔	✔
Ações maliciosas mais comuns:							
Altera e/ou remove arquivos	✔			✔			✔
Consome grande quantidade de recursos		✔	✔				
Furta informações sensíveis			✔	✔	✔		
Instala outros Códigos maliciosos		✔	✔	✔			✔
Possibilita o retorno do invasor						✔	✔
Envia *spam* e *phishing*			✔				
Desfere ataques na *internet*		✔	✔				

[11] Fonte: CERT.br (https://cartilha.cert.br/malware/).

Anexo VI – Autoridades e entes e órgãos reguladores e autorreguladores pertinentes

São autoridades e entes e órgãos reguladores e autorreguladores pertinentes com o que dispõe esta Política:

- ANBIMA: http://www.anbima.com.br;
- BACEN: http://www.bcb.gov.br;
- BSI Group: https://www.bsigroup.com/;
- B3: http://www.b3.com.br/pt_br/;
- CERT.br: https://www.cert.br/;
- CGI.br: https://cgi.br/;
- CVM: http://www.cvm.org.br;
- IEC: https://www.iec.ch/;
- IETF: https://ietf.org/;
- ISO: https://www.iso.org/home.html;
- UIF: http://fazenda.gov.br/orgaos/coaf; e
- RFB: http://www.fazenda.gov.br.

Anexo VII – Exemplos de Normas e diretrizes externas cujos dispositivos parcial ou totalmente aplicáveis

A presente Política está alinhada com dispositivos constantes das seguintes Normas e diretrizes:

• CAART:	Estabelece princípios e regras para o exercício da Atividade de Administração de Recursos de Terceiros;
• D5640:	Promulga a Convenção Internacional para Supressão do Financiamento do Terrorismo, adotada pela Assembleia-Geral das Nações Unidas;
• Guia ANBIMA de Cibersegurança, 2ª ed.:	Guia publicado no dia 6º do mês de dezembro do ano de 2017 pela ANBIMA, que descreve práticas efetivas para orientar a implantação de um programa de segurança cibernética e, com isso, objetiva contribuir para o aprimoramento da segurança cibernética nos mercados financeiro e de capitais do Brasil;
• Guia ANBIMA de PLD/FTP no Mercado de Capitais do Brasil:	Delineia diretrizes para o aprimoramento das práticas de PLD/FTP no mercado de capitais brasileiro;
• ICVM301:	Dispõe sobre a identificação, cadastro, registro, operações, comunicação, limites e responsabilidade administrativa referente aos crimes de lavagem de dinheiro ou ocultação de bens, direitos e valores;
• Resolução CVM 21:	Resolução número 21, de 25 de fevereiro de 2021 da Comissão de Valores Mobiliários da República Federativa do Brasil que dispõe sobre o Exercício Profissional de Administração de Carteiras de Valores Mobiliários.
• ISO/IEC 17799:2005:	Norma publicada no mês de junho do ano de 2005 pelo Isso em conjunto com a IEC, que estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos de controle e os controles definidos nesta norma têm como finalidade atender aos requisitos identificados na análise/avaliação de riscos;
• LGPD:	Lei Geral de Proteção de –ados - Lei n. 13.709, do dia 14 do mês de agosto do ano de 2018, da República Federativa do Brasil, que dispõe sobre generalidades de proteção de dados;
• L12527:	Lei do dia 18 do mês de novembro do ano de 2011, da República Federativa do Brasil que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei n. 8.112, de 11 de dezembro de 1990;

	revoga a Lei n. 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.
• L9613:	Dispõe sobre os crimes de lavagem de dinheiro ou ocultação de bens, direitos e valores; a preservação da utilização do sistema financeiro para o cometimento de tais atos ilícitos e, a criação da UIF; e
• RFC 2196 (The Site Security Handbook):	*Site Security Handbook* (Manual de Segurança de Sítio Eletrônico) emitido pela IETF conforme *o Request for Comment* (Requisição de Comentário) n. 2196.

Anexo VIII – Glossário

São os seguintes significados aqui pretendidos para os seguintes vocábulos:

• ANBIMA:	sigla para "Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais", sendo esta uma entidade que representa as instituições do mercado de capitais brasileiro;
• ANPD:	sigla para "Agência Nacional de Proteção de Dados";
• APT:	acrônimo para "*Advanced Persistent Threats*" (Ameaça Persistente Avançada);
• *Backdoor*:	termo para "método de escapar de uma autenticação ou criptografia normais em um sistema computacional, um produto ou um dispositivo embarcado (por ex. um roteador doméstico etc.), ou sua incorporação, por exemplo, como parte de um sistema criptográfico, um algoritmo, um *chipset* ou um 'computador homúnculo' (um pequeno computador dentro de outro)";
• *Backup*:	termo para "cópia de segurança";
• *Bots*:	diminutivo no plural de "robô", sendo esta, no ambiente informacional, uma aplicação de "software" concebido para simular ações humanas repetidas vezes e de maneira padrão;
• *Botnet*:	termo para "grupo de computadores conectados à *internet*, cada um deles rodando um ou mais 'bots' e se comunicando com outros dispositivos, a fim de executar determinada tarefa, como também uma "rede" de agentes de *software* ou *bots* que executam tarefas de maneira autônoma e automática, como, ainda, uma "rede" de computadores que utilizam software de computação distribuída";
• BS:	sigla para "*British Standards"*, sendo estes os padrões produzidos pelo BSI Group;
• BSI:	sigla para "*British Standards Institution"*, sendo este o órgão de padrões nacionais do Reino Unido;
• CAART:	sigla para "Código ANBIMA de Administração de Recursos de Terceiros";
• CERT.br:	sigla para "Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores no Brasil", sendo este um grupo de estudo do "CGI.br" e tendo por objetivo é auxiliar o Administrador de "redes" na gerência e implementação de soluções de segurança e, por premissa, que a segurança da informação é fundamental, e não deve ser isolada, portanto, de outras exigências da Tecnologia da Informação, necessitando o desenvolvimento de Processos para aumentar o nível da segurança;

• CGI.br:	sigla para "Comitê Gestor da Internet no Brasil", sendo esta uma estrutura multissetorial responsável por coordenar e integrar as iniciativas relacionadas ao uso e funcionamento da *internet* no Brasil criado pela Portaria Interministerial n. 147, de 31 de maio de 1995, da República Federativa do Brasil;
• *Chinese Wall*:	termo para "sistema físico, eletrônico e/ou lógico que visa impedir a circulação de informações que possam gerar conflito de interesses";
• Compliance:	termo para "o conjunto de disciplinas a fim de cumprir e se fazer cumprir as Normas legais e regulamentares, as políticas e as diretrizes estabelecidas para o negócio e para as atividades da instituição ou empresa, bem como evitar, detectar e tratar quaisquer desvios ou inconformidades que possam ocorrer";
• CVM:	sigla para "Comissão de Valores Mobiliários";
• DDoS:	acrônimo para "*Distributed Denial of Services*" ("Negação de Serviço Distribuído");
• Download:	termo para "transferir um ou mais arquivos de um 'servidor' remoto para um computador local";
• E-mail:	termo para "correio eletrônico";
• *Fax*:	Abreviatura de fac-símile", termo para "tecnologia de envio de documentos por linha telefônica";
• FI:	acrônimo para "Fundo de Investimento";
• *Firewall*:	termo para "sistema de segurança ou mecanismo desenvolvido para evitar que, através da *internet*, *hackers* ou programas de conteúdo duvidoso tenham acesso a um computador";
• *Hacker*:	termo para "pessoa que possui interesse e suficiente conhecimento em informática, sendo capaz de ingressar e modificar algum sistema informático mesmo que sem autorização";
• IEC:	sigla para "*International Electrotechnical Commission*" (Comissão Eletrotécnica Internacional), sendo esta uma organização internacional de padronização de tecnologias elétricas, eletrônicas e relacionadas;
• IETF:	sigla para "*Internet Engineering Task Force*" ("Força-Tarefa de Engenharia da Internet"), sendo este um grupo internacional aberto, composto de técnicos, agências, fabricantes, fornecedores e pesquisadores, que se ocupa do desenvolvimento e promoção de padrões para a *internet*;
• *Instant messenger*:	termo para "programa de mensagem instantânea";
• *Internet*:	termo para "'Rede' Mundial de Computadores";

• *Intranet*:	termo para "'rede' local de computadores, circunscrita aos limites internos de uma instituição, na qual são utilizados os mesmos programas e protocolos de comunicação empregados na *internet*;
• ISO:	sigla para "*International Organization for Standardization*" ("Organização Internacional para Padronização"), sendo esta uma entidade que congrega os grêmios de padronização e normalização de diversos países;
• *Know-how*:	termo para "conhecimento especializado";
• LDFTC:	sigla para "Lavagem de Dinheiro, Financiamento do Terrorismo e outros Crimes";
• LGPD:	sigla para "Lei Geral de Proteção de Dados" da República Federativa do Brasil;
• *Link*:	termo para "hiperligação eletrônica";
• *Log*:	termo para "Processo específico de registro de eventos relevantes num sistema";
• *Login*:	termo para "acesso a uma conta de serviço fornecido por um sistema informático";
• *Logoff*:	termo para "término do acesso a uma conta de serviço fornecido por um sistema informático";
• *Malware*:	termo para "*software* malicioso";
• Nuvem:	termo para "local genérico de armazenamento de dados acessível pela *internet*;"
• PCN:	sigla para "Plano de Continuidade de Negócios";
• *Pen drive*:	termo para "um tipo específico de dispositivo de memória facilmente portável fisicamente";
• *Pharming*:	termo para "cultivo do *phishing*";
• *Phishing*:	termo para "'pescaria' de dados";
• PLD/FTP:	sigla para "Programa de prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa";
• *Pop-ups*:	termo no singular para "um tipo de janela que se abre no navegador ao visitar uma página na *internet* ou ao acessar uma hiper ligação eletrônica específica";
• P2P:	acrônimo para "*peer to peer*" ("par-a-par");
• *Ransomware*:	termo para "*software* de sequestro de dados";
• Rede:	termo para "conjunto de dois ou mais dispositivos eletrônicos de computação (ou módulos processadores) interligados por um sistema de comunicação digital (ou *link* de dados), guiados por um conjunto de regras

	(protocolo de rede) para compartilhar entre si informação, serviços e, recursos físicos e lógicos”;
• RFB:	sigla para “Receita Federal do Brasil”, sendo esta a autoridade fiscal da República Federativa do Brasil;
• *Rootkit*:	termo para “coleção de *softwares* de computador projetada para permitir o acesso privilegiado a um computador ou a uma área do *software* não permitida oficialmente a um determinado usuário, bem como para ocultar Processos e arquivos específicos em algumas partes do sistema”;
• Servidor:	termo para “um *software* ou computador, com sistema de computação centralizada que fornece serviços a uma ‘rede’ de computadores”;
• *Website*:	termo para páginas virtuais disponibilizadas na *internet*;
• *Smishing*:	termo para “*phising* por texto”;
• *Software*:	termo para “programa de processamento de dados”;
• *Spam*:	termo oriundo do acrônimo utilizado para “*Sending and Posting Advertisement in Mass”* (“Enviar e Postar Publicidade em Massa”), por sua vez utilizado para referir-se a *e-mails* não solicitados e que geralmente são enviados sem um tratamento personalizado;
• *Spyware*:	termo para “*software* espião”;
• *Stakeholders*:	termo para “partes interessadas”;
• *Tablet*:	termo para “tipo de computador portátil, de tamanho pequeno, fina espessura e com tela sensível ao toque”;
• *Vishing*:	termo para “*phising* por voz”;
• *Wording*:	termo para “trabalho de escolha de termos para uma redação”; e
• *Worm*:	termo para “diferente de um vírus, um programa autorreplicante completo, não precisando de outro hospedeiro para se propagar”.