Política de Segurança da Informação e Segurança Cibernética

Área de Compliance
Versão 2022.1

Sumário

I – Documentos relacionados

Plano de Continuidade de Negócios	Definir as regras aplicáveis com base na estrutura da CIFI AM Brazil Ltda. (“CIFI AM”).

II – Sumário executivo

Objetivos da Política:

- Proteger os clientes, a imagem da CIFI AM e as informações pertencentes a ambos;
- Garantir a continuidade do negócio de forma que não haja interrupção dos serviços prestados aos clientes da CIFI AM;
- Reduzir os riscos de fraudes, espionagens, sabotagem, vandalismo, problemas causados por vírus, erros, uso indevido e roubo de informações e diversos outros problemas que possam comprometer os princípios básicos da segurança da informação; e
- Definir as regras aplicáveis com base na estrutura da CIFI AM.

Áreas de Atuação da CIFI AM:

- Consultoria de Valores Mobiliários nos termos da Resolução CVM 19/2021 (“Res. 19”).

Diretor Responsável por esta política: Carlos Rolando Poveda Castañeda

III – Introdução

Informação compreende qualquer conteúdo ou dado que tenha valor para uma determinada empresa ou pessoa e que possa ser armazenado, transferido ou manipulada de algum modo, servindo a determinado propósito (e.g., tomada de decisão). 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 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 CIFI AM exerce funções ligadas à consultoria de valores mobiliários, função esta que significa ter informações financeiras e protegidas por sigilo bancário. O acesso por pessoa não autorizada a informações e a perda, roubo ou a manipulação inadvertida destas podem gerar perdas significativas de imagem e danos financeiros, tanto para a CIFI AM quanto para seus clientes.

IV – Princípios básicos da segurança da informação

- **Confidencialidade**: limita o acesso a informação tão somente às pessoas ou instituições autorizadas pelo proprietário da informação;
- **Integridade**: garante que a informação manipulada 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 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 dos sócios e da diretoria da empresa quanto ao tema;
- Metodologia de classificação das informações para os colaboradores terem ciência da criticidade de cada informação;
- Conscientização dos usuários quanto a importância do tema; e

[1] O conceito de Segurança da Informação está padronizado pela norma ISO/IEC 17799:2005, influenciada pelo padrão inglês (British Standard) BS 7799.

[2] RFC 2196 (The Site Security Handbook)

- Implementação de um programa de segurança da Informação.

V – Classificação e ciclo das informações

V.1. Classificação das informações

V.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. 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 ou norma a CIFI AM é obrigada a divulgar publicamente, desde que não conflite com nenhuma lei que hierarquicamente seja superior.

V.1.2. Informações confidenciais

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

Desta forma, são consideradas informações confidenciais para a CIFI AM todo tipo de informação escrita, verbal ou apresentada de modo tangível ou intangível acessadas pelo colaborador em virtude do desempenho de suas atividades que possa incluir:

- Informações pessoais de clientes, contrapartes comerciais, fornecedores e prestadores de serviços (Lei 12.527/2011, art. 31);
- 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, dos clubes, fundos de investimento e carteiras geridas pela CIFI AM;
- Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento e carteiras que a CIFI AM atua como consultora;
- Estruturas e planos de ação;
- Qualquer informação relativa às atividades da CIFI AM, seus sócios ou seus clientes;
- Informações e recursos disponíveis a projetos e trabalhos críticos para a continuidade do negócio da organização; e
- Toda e qualquer informação que por força de lei seja obrigatório o sigilo e confidencialidade.

V.1.3. Informações reservadas

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

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

Logo, são consideradas informações reservadas todas as informações que:

- Sejam de áreas internas a CIFI AM que, por força de lei, norma ou ética, precisem ter segregação: (i) consultoria de valores mobiliários, e (ii) demais atividades da CIFI AM;
- Não possam ser acessadas por determinadas colaboradores e/ou áreas em função de trazerem risco de gerar conflito de interesse na tomada de decisão; e
- Sejam informações privilegiadas.

V.2. Ciclo das informações

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

- **Manuseio**: ocorre quando a informação é criada e/ou manipulada (e.g., ler uma apresentação impressa, digitar informações em um site, utilizar senha de acesso a um sistema);
- **Armazenamento**: a informação pode ser guardada em um banco de dados, papel, servidor ou dispositivo de armazenamento (e.g., nuvem, *pen-drive*, gaveta);
- **Transporte**: momento em que a informação é 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.

VI – Conscientização da importância da Política da segurança da informação

VI.1 – Treinamento, compreensão e adesão à política

Para (i) garantir os princípios da segurança da informação e (ii) os colaboradores entenderem a importância, é preciso assegurar que cada colaborador esteja em conformidade com as normas descritas nessa Política e nas leis que regem o setor de atuação da CIFI AM. 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, são necessários os 3 passos a seguir:

- Treinamento e compreensão a essa Política;
- Assinatura do Termo de Compromisso e Confidencialidade; e
- Reciclagem anual.

O cumprimento desses 3 passos é de responsabilidade do Diretor de Compliance, o qual seguirá as seguintes regras:

- 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 a ele 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 24 horas para que os colaboradores possam compreendê-las e observá-las integralmente no desempenho das suas respectivas atividades; e
- O programa periódico de reciclagem dos colaboradores tem a sua participação obrigatória, com o objetivo de fazer com que eles estejam sempre atualizados em relação às mudanças nas regras e atualizações de segurança da informação aplicáveis a CIFI AM.

VI.2 – Riscos de não cumprimento a esta Política

VI.2.1. Ataque cibernético

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.

Os invasores podem utilizar vários métodos para os ataques cibernéticos. Destacam-se os mais comuns (vide Anexo IV 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, softwares e banco de dados;
    - Cavalo de Troia: aparece dentro de outro *software* e cria uma porta para a invasão do computador;
    - *Spyware*: software malicioso para coletar e monitorar o uso de informações; e
    - *Ransomware*: *software* malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

- Engenharia social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:
    - *Pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;
    - *Phishing*: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
    - *Vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
    - *Smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e
    - Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.
- Ataques de DDoS (*distributed denial of services*) e *botnets* – ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos *botnets*, o ataque vem de muitos computadores infectados utilizados para criar e mandar *spam* ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.
- Invasões (*Advanced Persistent Threats* - APT) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

VI.2.2. Perda financeira

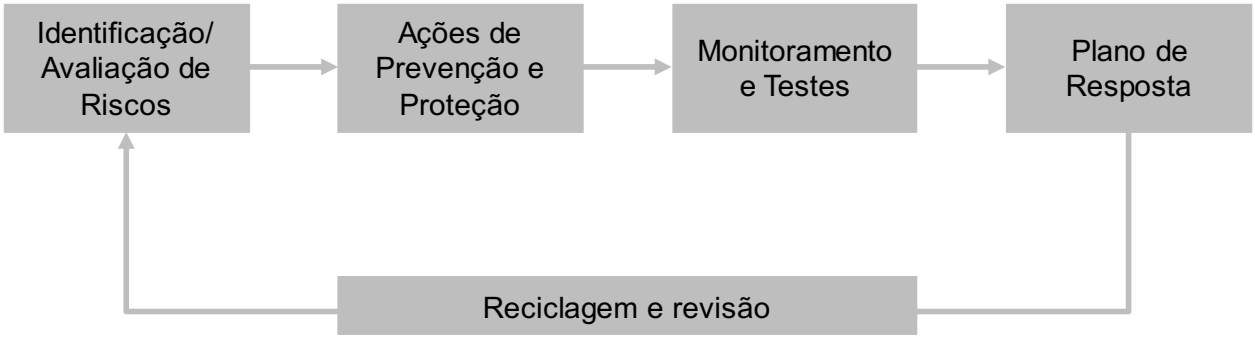
O não cumprimento dos princípios de segurança da informação (confidencialidade, integridade, disponibilidade e autenticidade) pode gerar perdas financeiras aos clientes e multas a CIFI AM por descumprimento a normas e leis.

VI.2.3. Risco de imagem e risco operacional

A perda de integridade, a não disponibilidade e a falta de autenticidade da informação podem gerar recomendações de investimento equivocada, o retardo nesta tomada, a perda do prazo de cumprimento de obrigações e, consequentemente, uma exposição negativa perante os *stakeholders*.

VII – Programa de segurança da informação

A CIFI AM adota um programa de segurança da informação que engloba os seguintes 5 (cinco) macro atividades:



VII.1 – Identificação/avaliação de riscos

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.

Forma de atuação: consiste em:

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

Todo esse ciclo do programa de segurança da informação é documentado na Matriz de Segurança das Informações.

VII.2 – Ações de prevenção e proteção

Objetivo: estabelecer e implementar medidas para mitigar e minimizar a concretização dos riscos identificados no item VII.1.

Forma de atuação: consiste em:

1. Implementar regras para manuseio, armazenamento, transporte e descarte (vide Anexo I);
2. Definir e implementar ações de proteção, prevenção e remediação das vulnerabilidades e riscos identificados na etapa acima (vide Matriz de Segurança das Informações e os anexos a esta política);
3. Treinar e conscientizar os colaboradores quanto a importância da segurança da informação (vide item VI e anexos a esta política).

VII.3 – Monitoramento e testes

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.

Forma de atuação: consiste em:

1. Monitorar a implementação e a execução das ações definidas no item VII.2 acima;
2. Monitorar semanalmente os relatórios de supervisão, logs e trilhas de auditória;
3. Monitorar semanalmente as rotinas de backup;
4. Monitorar quais equipamentos possuem acesso remoto aos dados e sistemas da CIFI AM;
5. Realizar anualmente testes de contingência e de restauração de dados;

Vide Matriz de Segurança da Informação e Anexo II.

VII.4 – Plano de resposta

Objetivo: ter um plano de resposta, tratamento e recuperação de incidentes, incluindo um plano de comunicação interna e externa, caso necessário.

Forma de atuação: consiste em:

1. Elaborar Plano de Continuidade de Negócios, atentando para a segurança e controles da contingência (vide Plano de Continuidade de Negócios);
2. Elaborar plano de resposta de acordo com a severidade quando da identificação da quebra de um ou mais dos princípios de segurança da informação (confidencialidade, integridade, disponibilidade e autenticidade) (vide Anexo III); e
3. Arquivar documentos relacionados ao programa de segurança da informação por 5 (cinco) anos.

VII.5 – Reciclagem e revisão

Objetivo: manter o programa de segurança da informação continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

Forma de atuação: consiste em:

1. Instituir Comitê de Segurança da Informação (vide item VIII – Governança, abaixo);
2. Elaborar relatório anual de segurança da informação; e
3. Revisar anualmente ou sempre que o Comitê de Segurança da Informação achar necessário.

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

A.I.1 – Política de e-mails

- Não abra anexos com as extensões .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;
- Desconfie de todos os e-mails com assuntos estranhos e/ou inglês. Exemplos: ILOVEYOU, Branca de Neve Pornô, Veja as fotos da XX, ganhe dinheiro sem sair de casa, sua senha do banco será revogada, seu nome será negativado;
- Não acesse e-mails pessoais pelos computadores, celulares, tablets ou qualquer outro equipamento da CIFI AM ou utilizando a sua rede/internet;
- O e-mail da CIFI AM é de uso estritamente profissional, não devendo ser utilizado para fins pessoais;
- Os colaboradores não poderão usar intencionalmente o e-mail da CIFI AM 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 Controles internos imediatamente;

A.I.1.1. Aviso em e-mail

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

> This message and its attachments are confidential, privileged, and otherwise protected from disclosure. If you are not the intended recipient, you may not use, copy, or disclose the contents of this message and its attachments. If received in error, please contact the sender immediately and delete this message from your system. Thank you.
>
> Esta mensagem e seus anexos são confidenciais, privilegiados e protegidos da divulgação. Se você não for o destinatário pretendido, você não poderá usar, copiar ou divulgar o conteúdo desta mensagem e seus anexos. Se for recebido por engano, entre em contato com o remetente imediatamente e exclua esta mensagem do seu sistema. Obrigado.

A.I.2 – Política de senhas

- Utilize sempre senhas alfanuméricas (letras e números) com diferentes caixas (maiúscula e minúscula) e caracteres especiais;

- Mantenha sua senha sempre segura e não a revele a ninguém e nem a deixe anotada em qualquer lugar em que possa ser facilmente descoberta;
- Tudo que for executado com sua senha será de sua inteira responsabilidade, excetuando casos comprovadamente de vulnerabilidades da infraestrutura de segurança da informação;
- Não utilize senhas fáceis de serem descobertas, tais como nome da esposa, dos filhos, datas comemorativas pessoais.

A.I.3 – Política de internet

- A internet da CIFI AM é de uso estritamente profissional, não devendo ser utilizada para fins pessoais. Os colaboradores não poderão entrar em sites com conteúdo ofensivo, inadequado ou que promova qualquer tipo de discriminação racial, social ou moral;
- É proibido o uso de ferramentas P2P (kazaa, Morpheus, etc);
- É proibido o uso de instante messengers não homologados/autorizados pela área de Compliance;
- Monitoramento: a área de Controles Internos poderá monitorar os sites 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. Isso significa que tudo o que venha a ser executado de sua estação acarretará em responsabilidade sua. Por isso, sempre que sair da frente da estação, tenha certeza de que efetuou o *logoff* ou travou o console.

A.I.4.1. Instalação e *download* de *softwares*

Todo *software* somente poderá ser instalado mediante autorização da área de suporte. Caso seja necessário fazer algum *download*, o colaborador deverá solicitar autorização prévia junto a Área de Compliance.

Download de aplicativos: é proibido baixar qualquer tipo de *software* não autorizado pela área de suporte em função de aplicativos não autorizados poderem abrir brechas no *firewall* da CIFI AM.

A.I.4.2. Proteção antivírus

O servidor e os computadores da CIFI AM 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 a organização.

A renovação da licença do antivírus é realizada automaticamente.

A.I.5. Política social

- Não fale sobre a Política de segurança da informação ou sobre qualquer item relacionada a ela com terceiros que não tenham autorização sobre o assunto ou em locais públicos;
- Não diga sua senha para ninguém. Qualquer colaborador da CIFI AM jamais irá pedir sua senha;
- Não digite suas senhas em máquinas que não sejam da CIFI AM;
- Caso digite sua senha em uma estação de trabalho que não seja sua, certifique-se que a opção de guardar sua senha esteja desabilidade para o serviço;
- Não passe informações da CIFI AM para pessoa não identificada ou desconhecida, mesmo que ela se apresente como sendo colaborador de empresa ou associação que a CIFI AM tenha relacionamento;
- Relate a área de Compliance pedidos internos e externos que venham a conflitar com qualquer item desta política.

A.I.6. Política de segregação de atividades

A consultoria de valores mobiliários deve ser segregada das demais atividades exercidas pela pessoa jurídica, por meio da adoção dos seguintes procedimentos:

A.I.7.1. *Chinese Wall*

Com a finalidade de se evitar o uso e o acesso a informações privilegiadas, confidenciais ou reservadas, o grupo a qual pertence a CIFI AM utiliza-se do conceito *Chinese Wall*, o qual segrega as informações de colaboradores envoltos em atividades de consultoria de valores mobiliários e as demais atividades desempenhadas pelo grupo.

Este muro de informações é controlado e mantido pelo Diretor de Compliance, o qual se incumbe de manter a integridade da segregação, através da supervisão das atividades.

A comunicação entre as áreas separadas pelo *Chinese Wall* é feita como se fossem de empresas distintas, seguindo as normas desta Política de segurança da informação e do Manual de compliance.

A.I.7.2. Criação e manutenção de usuários

Os acessos internos e externos aos serviços de rede da CIFI AM são liberados de acordo com a função que o colaborador exerce na empresa e de acordo com a sua necessidade. A área de suporte é a responsável por definir os acessos de todos os colaboradores.

Quando da troca de função dentro da empresa, a área de suporte é obrigada a ser avisada imediatamente e os acessos revistos em função do exercício da nova função.

Quando do desligamento de colaboradores, o seu acesso à rede e e-mail é revogado a partir do momento que o desligamento for informado à área de suporte.

A.I.8. Política de manuseio, armazenamento e descarte de arquivos

Todo e qualquer arquivo, documento, relatório, pesquisa, banco de dados, sistema e planilha da CIFI AM deverá ser salvo na rede.

A CIFI AM deve manter digitalmente, pelo prazo mínimo de 5 (cinco) anos após o fim do relacionamento com o cliente, ou por prazo superior por determinação expressa da CVM, todos os documentos e informações exigidos pela CVM, bem como toda a correspondência, interna e externa, todos os papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções.

É de responsabilidade de todos os colaboradores gravar e manter as informações da **CIFI AM** na rede.

A.I.8.2. Realização de cópias de segurança

Cópias de segurança dos dados do servidor e da nuvem são feitas diariamente e mantidas na nuvem. A Área de Controles Internos verifica semanalmente se a cópia está sendo executada.

A.I.8.3. 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.
Login de acesso	Devem ter sua senha e login revogados e depois excluídos.

A.I.9. Política de transporte de informações confidenciais

É terminantemente proibido aos colaboradores fazerem cópias (físicas ou eletrônicas) de arquivos contendo informações confidenciais ou não de propriedade da CIFI AM e circular em ambientes externos à empresa ou dar acesso a colaboradores não autorizados com estes arquivos sem a devida autorização da área de Compliance.

A.I.9.1. *Firewall*

Alteração da configuração do firewall: somente os colaboradores habilitados podem proceder com qualquer alteração da configuração do firewall.

Monitoramento do firewall: é de responsabilidade da área de Controles Internos o monitoramento do firewall da empresa.

A.I.9.2. Acesso remoto à rede

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

Em função das regras legais e das informações confidenciais que a CIFI AM manuseia e o risco do transporte dessa informação para fora de sua rede, devem ser observadas as seguintes regras:

- A conexão remota deve ser feita com segurança de dados em ambos os lados;
- A regras de segurança de dados devem ser definidas e revisadas pelo Comitê de Segurança da Informação;
- Todos os acessos remotos devem ser aprovados pelo Diretor de Compliance ;
- O controle das regras de segurança de dados deve ser feito por controles internos.

A.I.10. Avisos importantes em apresentações

Toda apresentação a clientes, contrapartes comerciais, fornecedores e prestadores de serviços que contenham informações classificadas como confidenciais deve conter:

- Aviso que o material é confidencial e de propriedade da CIFI AM; e
- Todas as páginas devem conter a mensagem de “informação confidencial” ou “Confidencial”.

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

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 CIFI AM BRAZIL se reserva no direito de rastrear, monitorar, gravar e inspecionar todos e qualquer tráfego de voz realizado através de contato telefônico e internet, bem como troca de informações escritas transmitidas via: 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 a CIFI AM ou utilizados em nome dela.

A.II.1.2. Monitoramento da rede

Trilhas de auditoria registrando as exceções e outros eventos de segurança relevantes:

- Produzidas e mantidas por um período determinado pela área de Compliance;
- É de responsabilidade da área de Controles internos 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-se monitorar os acessos a estes, incluindo erro de senhas e atividades desempenhadas.

Para os sistemas e infraestrutura disponibilizada por *vendors*, deve-se verificar a execução de auditorias e inspeções nos registros e verificação se os sistemas são protegidos contra adulterações.

A.II.1.4. Monitoramento de acesso à rede

Consiste em:

- Verificar quem acessa a rede e se acessa as informações que tem a permissão de acessar;
- Verificar se houve acesso indevido de pessoa não autorizada na rede.

Anexo III – Gestão de incidentes de segurança da informação

Qualquer política de segurança da informação e controles propostos por um Programa de Segurança da Informação mitigam riscos relacionados à segurança, mas não garantem a proteção total dos ativos.

Em menor ou maior escala, as vulnerabilidades residuais existem e podem tornar ineficaz a proteção à informação. 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. Segundo CERT.br[3], 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. Exemplo: o e-mail contendo informações confidenciais ou sensíveis enviadas para destinatários incorretos;
- Roubo ou perda de informações confidenciais. Exemplo: cópia impressa de informações confidenciais ou reservadas roubadas ou esquecidas em lugar de livre circulação de pessoas;
- Modificação não autorizada de informações confidenciais ou reservadas;
- Roubo ou perda de equipamento que contenha informações confidenciais ou acesso a elas. Exemplo: tablet, celulares ou notebook contendo informações confidenciais com acesso a rede da CIFI AM;
- A desconfiguração do portal web da CIFI AM;
- A propagação de um vírus ou worm por meio da lista de contatos de e-mails;
- Envio de spam;
- Seu equipamento está repentinamente muito lento;
- Há notificações estranhas;
- Você vê muito pop-ups quando navega;
- Seu equipamento tem arquivos que você nunca viu antes;
- Você perdeu arquivos, seu disco rígido foi parcialmente ou completamente apagado;
- Sua homepage mudou;
- Seu navegador tem uma nova barra de ferramentas que você não solicitou;
- Amigos e colegas avisam que eles estão recebendo e-mails estranhos de você;
- Seu antivírus não atualiza mais ou fornece mensagens de erro obscuras;

[3] Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil

O Processo de Gestão de Incidentes mostra grande variação em sua implementação. Ela depende muito do tamanho da empresa, da complexidade das atividades exercidas e da regulamentação a que a empresa é obrigada a seguir.

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 notificação, 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, relate-a para um dos membros do Comitê de Segurança da Informação.

Todos os procedimentos e checklist das atividades a serem desempenhadas em um caso de incidente estão detalhados na Matriz de Segurança da Informação.

Anexo IV – Resumo comparativo entre códigos maliciosos[4]

Códigos Maliciosos							
	Vírus	*Worm*	*Bot*	*Trojan*	*Spyware*	*Backdoor*	*Rootkit*
Como é obtido:							
Recebido automaticamente pela rede		✓	✓				
Recebido por *e-mail*	✓	✓	✓	✓	✓		
Baixado de *sites* 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			✓	✓	✓		

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

Instala outros códigos maliciosos		✓	✓	✓			✓
Possibilita o retorno do invasor						✓	✓
Envia *spam* e *phishing*			✓				
Desfere ataques na Internet		✓	✓				
Procura se manter escondido	✓				✓	✓	✓

Anexo IV – Procedimentos de Dados Pessoais

A.IV.1. Procedimentos Solicitados pelos Clientes

- ANONIMIZAÇÃO: 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, a um indivíduo;
- CONSENTIMENTO: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
- BLOQUEIO: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
- ELIMINAÇÃO: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
- TRANSFERÊNCIA INTERNACIONAL DE DADOS: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
- PORTABILIDADE
- TRATAMENTO AUTOMATIZADO
- COPIA DOS DADOS

A.IV.2. Procedimentos Solicitados 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.

Anexo VI – Controle de versão

Versão	Data	Nome	Ação (Elaboração, Revisão, Alteração)	Conteúdo
2022.1	10/05/2022	IGMC	Elaboração	Primeira versão do documento.
	10/05/2022	Diretoria CIFI AM – Diretor de Compliance	Aprovação	Entrada em vigor: 20/05/2022