AMARIL FRANKLIN

Corretora de Títulos e Valores Ltda

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SUMÁRIO

1. OBJETIVO

São objetivos da Política de Segurança da Informação:

- Garantir a confidencialidade, a privacidade, a integridade, a legalidade e autenticidade das informações de propriedade da Amaril Franklin Corretora de Títulos e Valores Ltda e/ou a nós confiados.
- Assegurar a disponibilidade dos dados e sistemas de informação utilizados pela Amaril Franklin Corretora de Títulos e Valores Ltda.
- Prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, definindo estratégias para aplicação das regras de segurança da informação.
- Demonstrar o compromisso da Amaril Franklin Corretora de Títulos e Valores Ltda em zelar pela segurança e privacidade das informações de seus clientes.
- Reafirmar o nosso compromisso com os aspectos regulatórios das principais regulamentações vigentes.

2. VIGÊNCIA

Esta Política pode ser revisada anualmente ou, quando necessário. A Revisão pode ocorrer em caso de mudanças de tecnologia, nas normas e diretrizes da Amaril Franklin Corretora de Títulos e Valores Ltda que impactem a segurança da informação ou se requerido por algum órgão regulador.

3. ÁREAS DE APLICAÇÃO

Todas as áreas da Amaril Franklin Corretora de Títulos e Valores Ltda, incluindo prestadores de serviço.

4. PRINCÍPIO DE SEGURANÇA DA INFORMAÇÃO

Acreditamos que a informação é o bem mais importantes no mercado financeiro, dessa forma, os princípios de segurança da informação que tem como objetivo a preservação da propriedade da informação (confidencialidade, integridade e disponibilidade), permitindo apenas o uso e compartilhamento de forma controlada é atendido através do monitoramento dos dados e de seu compartilhamento, além do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

Vale ressaltar que:

- Confidencialidade: As informações sejam de conhecimento exclusivo de pessoas especificamente autorizadas;
- Integridade: As informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais;
- Disponibilidade: As informações estejam disponíveis a todas as pessoas autorizadas.

5. ESTRUTURA DE GERENCIAMENTO DE SEGURANÇA CIBERNÉTICA

Todo o gerenciamento dos controles de segurança foi desenvolvido e ajustado para garantir que os procedimentos operacionais sejam desenvolvidos, implantados e mantidos ou modificados de acordo com Política de Segurança da Informação.

Ressaltamos assim que as precauções na utilização de produtos e serviços financeiros, descritas nesta política são fundamentais para a segurança das operações, assim como conhecer os produtos e serviços financeiros que serão contratados pelo Cliente.

5.1 Gestão de acessos às informações

Os acessos as informações são controlados e monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente, e cancelados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço.
É considerado como informação sensível todo e qualquer dado de clientes, de operações e posições de custódia que permitam ou não a identificação do Cliente.

A liberação de acesso à rede e sistemas deve ser aprovada pelo responsável do sistema. A área de TI, como responsável por toda a rede e a responsável por realizar a liberação do acesso, poderá a seu critério, dar acesso aos fornecedores contratados os acessos necessários para a realização de suas atividades. Para novos usuários de colaboradores é necessário receber a informação da área de Recursos Humanos informando que a contratação já foi finalizada para dar os devidos acessos.

Os servidores da Amaril Franklin Corretora de Títulos e Valores Ltda são mantidos em áreas seguras, com controle de acesso, incluindo proteção contra ameaças físicas e ambientais.

Os colaboradores, prepostos e prestadores de serviços são orientados, sobre os conceitos de Segurança da Informação, para conscientização e disseminação da cultura de segurança cibernética através do nosso Programa de Conscientização de Segurança da Informação, o qual deve possuir frequência mínima anual e ser atualizado sempre que se fizer necessário.

O Programa de Conscientização de Segurança da Informação, para atingir o objetivo de uma maior cultura segurança cibernética, deve tratar de informações sobre: Dados sensíveis, Comunicação de incidente, a guarda de documentação e a segregação de dados e controle de acesso.

5.2 Proteção do ambiente de rede

Existem controles e responsabilidades pela gestão e operação dos recursos tecnológicos para processamento das informações, que visam garantir a segurança na infraestrutura tecnológica por meio do gerenciamento efetivo no monitoramento, tratamento e na resposta aos incidentes, com o intuito de minimizar o risco de falhas e a administração segura de redes de comunicações.

5.2.1 Gestão de Incidentes de Segurança da Informação

O comportamento de possíveis ataques é identificado por meio de controles de detecção implementados no ambiente, como filtro de conteúdo aos quais os colaboradores possuem acesso, Antivírus, ferramenta de detecção de comportamentos maliciosos, AntiSpam, entre outros.

5.2.2 Prevenção a Vazamento de Informações

Utilização de controle para prevenção de perda de dados, responsável por garantir que dados confidenciais não sejam perdidos, roubados, mal utilizados ou vazados na web por usuários não autorizados.

5.2.3 Avaliação de Ameaças e Vulnerabilidades

As verificações das redes internas e externas devem ser executadas periodicamente, no mínimo anualmente. As vulnerabilidades identificadas devem ser tratadas e priorizadas de acordo com seu nível de criticidade.

5.2.4 Controle Contra Software Malicioso

Todos os equipamentos (computadores, servidores, etc) que estejam conectados à rede corporativa, devem, sempre que compatível, ser protegidos com uma solução antimalware determinada pela área de Segurança da Informação e verificação periódica dos softwares instalados.

5.2.5 Rastreabilidade

Trilhas de auditoria devem ser implantadas para todos os componentes de sistema para reconstruir os seguintes eventos:

- Autenticação de usuários (tentativas válidas e inválidas);
- Acesso a informações;
- Ações executadas pelos usuários, incluindo criação ou remoção de objetos dos sistemas.

5.2.6 Segmentação de Rede

- Computadores conectados à rede corporativa não devem ser acessíveis diretamente pela Internet, somente poderão ser acessados via aplicativos de acesso remoto e VPN autorizados pelo setor de TI.
- Não é permitida a conexão direta de rede de terceiros utilizando-se protocolos de controle remoto aos servidores conectados diretamente na rede corporativa;
- Para solicitação de criação, alteração e exclusão de regras nos firewalls e ativos de rede, o requisitante deve encaminhar pedido à área de TI, que fará a análise e aprovação.
- A página da Amaril Franklin Corretora de Títulos e Valores Ltda, na rede mundial de computadores, incluindo os sistemas que dão acessos aos clientes, devem possuir certificados de segurança e criptografia, permitindo acesso apenas via protocolo HTTPs.

5.2.7 Cópias de Segurança (Backup)

O processo de execução de backups é realizado diariamente, de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes.

A Amaril Franklin Corretora de Títulos e Valores Ltda mantém uma Política de Backup para tratar de forma específica este assunto, a qual define como e quando os backups devem ocorrer. A Política de Backup deve ser revisada sempre que os procedimentos de Backup precisarem ser alterados devido a mudanças de tecnologia ou em caso de mudança nas normas e diretrizes da Amaril Franklin Corretora de Títulos e Valores Ltda que impactem o processo ou se requerido por algum órgão regulador.

5.2.8 Plano de Ação de respostas a incidentes

Para cada possível incidente identificado pela Amaril Franklin Corretora de Títulos e Valores Ltda, a área de TI, possuí um documento interno (Plano de Ação e Resposta a Incidentes) com o mapeamento dos processos a serem executados, pela Amaril Franklin Corretora de Títulos e Valores Ltda ou empresa terceira contratada, com o objetivo final de lidar com a situação de modo a limitar os danos ao negócio e especialmente ao cliente, reduzindo o tempo e os custos de recuperação. Esse documento deve ser constantemente atualizado para refletir os processos atuais e as melhores práticas de segurança.

Para elaboração do “Plano de Ação e Resposta a Incidentes”, deverá ser considerado diversos cenários para garantir a continuidade dos negócios, tais como, não se limitando, queda de energia, perda de links de internet, falhas de sistemas ou servidores. Além disso cada plano deverá ser classificado:

- Categoria do incidente: Tipo de evento que levou a abertura do incidente
- Impacto de funcionamento: Qual o impacto do evento para o funcionamento dos serviços internos e externos
- Impacto da informação: Como as informações armazenadas serão impactadas.
- Esforço de recuperação: Definição do esforço estimado para retorno a situação normal.
- Probabilidade de ocorrência: Definição da probabilidade de o incidente mapeado ocorrer.

Os planos devem conter os procedimentos de comunicação as demais áreas da Amaril Franklin Corretora de Títulos e Valores Ltda e em caso de incidentes que afetem um ou mais clientes, a área responsável pelo serviço prestado deverá comunicar aos clientes afetados.

Juntamente com o “Plano de Ação e Resposta a Incidentes” deverá ser mantido o Controle de Incidentes Relevantes que deverá conter no mínimo a Data do Incidente, o tipo de incidente, a Descrição do Incidente, a Data de Retorno a situação normal e o Plano de Ação para evitar que incidentes semelhantes voltem a ocorrer, a categoria do incidente, a criticidade do incidente, o impacto de funcionamento, impacto da informação e o esforço de recuperação.

Ao final de cada ano, conforme Resolução Nº 4.658 do Banco central, a área de TI deverá elaborar o Relatório anual sobre a implementação do Plano de ação e de resposta a incidentes e aprovar junto a Diretoria da Amaril Franklin Corretora de Títulos e Valores Ltda.

5.2.9 Vulnerabilidade contra ataques cibernéticos

O sistema de Firewall da Amaril Franklin Corretora de Títulos e Valores Ltda deve realizar o monitoramento online contra os ataques cibernéticos, impedindo as tentativas e gerando os alertas de invasão que são enviados para a área de TI.

É necessário a contratação de uma empresa especializada em Firewall para monitoração em tempo hábil e atualização do Firewall.

A implementação, a aplicação e a eficácia das medidas adotadas para reduzir a vulnerabilidade contra os ataques cibernéticos devem ser controladas através do documento interno “Plano de Ação e Resposta a Incidentes”.

As verificações das vulnerabilidades contra ataques cibernéticos devem ser executadas e revisadas periodicamente, no mínimo anualmente, para permitir a identificação de novos riscos cibernéticos. Além disso, é fundamental que tanto os fornecedores contratados, quanto a área de TI interna acompanhe fóruns, treinamentos e relatórios que possibilitem o compartilhamento de informações sobre ameaças e vulnerabilidades relevantes, conforme item 6.5 Identificação de Vulnerabilidades.

5.3 Confidencialidade e integridade da informação

As informações que não sejam de domínio público e que tenham sido obtidas pelo fato de a pessoa trabalhar na Amaril Franklin Corretora de Títulos e Valores Ltda não podem ser usadas para auferir ganhos pessoais ou de qualquer outra pessoa que esteja associada de alguma forma a este colaborador.

Os colaboradores que tenham acesso aos dados de clientes comprometem-se a mantê-los sob a mais estrita confidencialidade.

É responsabilidade da sociedade e seus colaboradores executar os meios de segurança suficientes para proteger a informação reservada e confidencial, conforme preceitua as boas práticas do mercado.

A Amaril Franklin Corretora de Títulos e Valores Ltda poderá revelar as informações confidenciais nas seguintes hipóteses:

- Quando for obrigado a revelá-las, em virtude de dispositivo legal, ato de autoridade competente, ordem ou mandado judicial;
- Aos órgãos de proteção e defesa de crédito e prestadores de serviços autorizados pela Amaril Franklin Corretora de Títulos e Valores Ltda a defender seus direitos e créditos;
- Aos órgãos reguladores do mercado financeiro;
- Para outras instituições financeiras, desde que dentro dos parâmetros legais estabelecidos para tanto, podendo, nesta hipótese, o cliente, a qualquer tempo, cancelar sua autorização.

5.4 Autenticação e Senha

O acesso às informações e aos ambientes tecnológicos deve ser permitido apenas às pessoas autorizadas pelo Proprietário da Informação, levando em consideração o princípio do menor privilégio, a segregação de funções conflitantes e a classificação da informação.

5.4.1 Nos sistemas internos

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

- Credenciais de acesso individualizados, monitorados e passíveis de bloqueios e restrições (automatizados e manuais);
- Remoção de autorizações dadas a usuários afastados ou desligados da Amaril Franklin Corretora de Títulos e Valores Ltda, ou ainda que tenham mudado de função; e
- A revisão periódica das autorizações concedidas.

A senha a ser escolhido pelo usuário e gravado nos sistemas é de uso pessoal, intransferível e de conhecimento exclusivo.

Sendo de inteira responsabilidade do usuário todo e qualquer prejuízo causado pelo fornecimento de sua senha pessoal a terceiros, independente do motivo.

5.4.2 Pelos Clientes

O cliente é responsável pelos atos executados com seu usuário (login), que é único e acompanhado de senha exclusiva para autenticação individual no acesso à informação e aos recursos de tecnologia. Recomendamos que:

- Evite anotar em papel ou contar a alguma pessoa, para manter a confidencialidade memorize sua senha.
- Alterar a senha sempre que existir qualquer suspeita do comprometimento dela;
- Elaborar senhas de qualidade, de modo que sejam complexas e de difícil adivinhação;
- Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação;
- Bloquear sempre o equipamento ao se ausentar.
- Essas recomendações valem também para o seu e-mail cadastrado na Amaril Franklin Corretora de Títulos e Valores Ltda o qual permite efetuar a troca de senhas.

5.4.3 Parâmetros de senha

- As senhas de acesso à rede e aos sistemas internos devem conter no mínimo os seguintes parâmetros:
- Tamanho mínimo: 6 caracteres;
- Tempo máximo de expiração: 45 dias;
- Quantidade máxima de tentativas antes do bloqueio: 3;
- Duração do bloqueio: desbloqueio pelo administrador;
- Histórico mínimo de senhas utilizadas: 6;
- Complexidade: ativada; e
- Serem criptografadas.

5.5 Antivírus e Proteção

5.5.1 Nos sistemas internos

Todos os computadores e servidores da Amaril Franklin Corretora de Títulos e Valores Ltda, terão sistemas de Antivirus instalado e atualizado a todo momento, a área de TI realiza o monitoramento em tempo real para verificação do seu correto funcionamento, incluindo sua ativação, atualização e varredura de sistema.

Além disso, a área de TI, também acompanha as atualizações dos sistemas operacionais e dos Softwares instalados das máquinas e servidores, garantindo a instalação das últimas versões que permitem uma maior segurança do sistema em até 90 dias da disponibilização das atualizações, tempo este utilizado para realizar a homologação das atualizações.

5.5.2 Pelos Clientes

Recomendamos que o cliente mantenha uma solução de antivírus atualizada e instalada no computador utilizado para acesso aos sistemas oferecidos pela Amaril Franklin. Além disso, possuir o sistema operacional atualizado com as últimas atualizações realizadas.

5.6 Utilização da Internet

É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações sigilosas em listas de discussão ou bate-papo;

Todos os downloads de programas da Internet que sejam necessários ao desempenho das atividades do colaborador deverão ser realizados por um profissional da área de TI.

O usuário deve utilizar a Internet de forma adequada e diligente;

O usuário deve utilizar a Internet observando a conformidade com a lei, a moral, os bons costumes aceitos e a ordem pública;

O usuário deve se abster de utilizar a Internet com objetivos ou meio para a prática de atos ilícitos, proibidos pela lei ou pela presente norma, lesivos aos direitos e interesses da Amaril Franklin Corretora de Títulos e Valores Ltda ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros;

5.7 Utilização do Correio Eletrônico (E-mail)

Todos os usuários que utilizarem esse serviço deverão fazê-lo no sentido de evitar o comprometimento da imagem ou que cause prejuízo moral ou financeiro da Amaril Franklin Corretora de Títulos e Valores Ltda, perante seus clientes e comunidade em geral, mantendo uma conduta profissional, especialmente em se tratando da utilização do bem público.

Todas as contas de correio eletrônico terão uma titularidade, determinando a responsabilidade sobre a sua utilização;

Os usuários poderão ser titulares de uma única caixa postal individual no Servidor de Correio Eletrônico, com direitos de envio/recebimento de mensagens, via Intranet e Internet.

Contas com inatividade (sem envio e-mails validos) por um período igual ou superior a 60 (sessenta) dias serão bloqueadas, a fim de evitar acessos indevidos.

Contas com inatividade (sem envio e recebimento de e-mails validos) por um período igual ou superior a 120 dias serão excluídas, a fim de evitar o recebimento de novas mensagens. O histórico de e-mails enviados e recebidos de todas as contas sempre será salvo.

O usuário é o responsável direto pelas mensagens enviadas por intermédio do seu endereço de correio eletrônico;

O usuário deve utilizar o correio eletrônico de forma adequada e diligente;

É vedada a utilização do correio eletrônico, nas situações abaixo:

- Acesso não autorizado à caixa postal de outro usuário;
- Envio, armazenamento e manuseio de material que contrarie o disposto na legislação vigente, a moral e os bons costumes e a ordem pública;
- Envio, armazenamento e manuseio de material que caracterize a divulgação, incentivo ou prática de atos ilícitos, proibidos pela lei ou pela presente Norma, lesivos aos direitos e interesses da sociedade ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, do usuário ou de terceiros;
- Envio, armazenamento e manuseio de material que caracterize: promoção, divulgação ou incentivo a ameaças, difamação ou assédio a outras pessoas; assuntos de caráter obsceno; prática de qualquer tipo de discriminação relativa à raça, sexo ou credo religioso; distribuição de qualquer material que caracterize violação de direito autoral garantido por lei; uso para atividades com fins comerciais e o uso extensivo para assuntos pessoais ou privados;
- Envio de mensagens do tipo “corrente” e “spam”;
- Envio intencional de mensagens que contenham vírus eletrônico ou qualquer forma de rotinas de programação de computador, prejudiciais ou danosas;
- Envio de mensagens que contenham arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança de acordo com os critérios estabelecidos pela Amaril Franklin Corretora de Títulos e Valores Ltda.

- Utilização de listas de e-mail da Amaril Franklin Corretora de Títulos e Valores Ltda para a distribuição de mensagens que não sejam de estrito interesse funcional e sem a devida permissão do responsável pelas listas e/ou caderno de endereços em questão.

O Setor de TI e a Diretoria poderão ter acesso ao conteúdo dos e-mails, sempre que for avaliado o melhor interesse da Amaril Franklin Corretora de Títulos e Valores Ltda.

5.8 Utilização de software

Nenhum software poderá ser instalado na Amaril Franklin Corretora de Títulos e Valores Ltda, se não estiver homologado pela área de Informática, exceto nos casos de pesquisa dessa área antes da referida homologação.

Somente o setor de TI possuí permissão para a instalação de qualquer software, mesmo que já homologado e de uso público.

5.9 Segurança física dos ambientes de operação e processamento

A segurança física tem por objetivo prevenir o acesso físico não autorizado, danos às instalações, fraude ou sabotagem entre outras ameaças. Convém que as instalações de processamento da informação críticas sejam mantidas em áreas seguras, protegidas por perímetros de segurança.

As áreas de operações e processamento deverão estar protegidas por dispositivos de segurança e placas indicativas de restrição de acesso.

6. GERENCIAMENTO DE RISCOS DE TI

O Gerenciamento de Riscos de TI tem como objetivo alcançar um equilíbrio entre os riscos e custos de operações. Uma boa gestão de riscos possibilita tomadas de decisões mais assertivas, tornando as atividades operacionais menos sujeitas a interrupções e paradas devido a ataques ou erros no sistema.

Assim esta política visa montar uma estratégia de gerenciamento de risco e definir os critérios (inclusive os já descritos no item “5.2.8 - Plano de Ação de respostas a incidentes”) que serão adotados para a avaliação, resposta e monitoramento dos riscos.

Para o contexto dessa política, atualizações de sistemas fornecidos por terceiros deverão ser homologados, com o objetivo de reduzir os riscos na implementação, mas não serão considerados como projetos de melhoria, portanto não estarão descritos como Planos de Ação/Melhorias.

6.1 Os Riscos em TI

No documento interno de “Plano de Ação e Respostas a Incidentes”, deverá constar os **Riscos envolvidos na não implementação** e os **Riscos envolvidos na Implantação** em cada projeto de Melhoria elaborado.

Esses riscos podem ser relacionados a 3 cenários:

- Risco de oportunidade: Perda de oportunidades do uso da TI como uma forma de melhoria na eficiência dos processos.
- Risco de entrega de projetos: Qualidade, relevância e performance do projeto desenvolvido.
- Riscos operacionais e de entrega do serviço: Performance dos serviços e sistemas de TI, envolvendo problemas como a interrupção dos sistemas, problemas de segurança e outras complicações.

É importante ressaltar, na elaboração dos projetos e tomada de decisões deve ser levada em consideração que o nível de risco em projetos de TI varia de acordo com:

- Tamanho: os riscos são diretamente proporcionais ao tamanho do projeto, e crescem junto com o orçamento, tamanho da equipe, tempo de implementação e áreas organizacionais afetadas.

- Estrutura: os processos são mais claros, diretos e bem definidos em projetos bem estruturados.
- Experiência com tecnologia: os riscos no projeto são inversamente proporcionais ao nível de experiência da equipe envolvida.

6.2 Aceitação de Riscos

Ainda que todas as medidas sejam tomadas, todo projeto sempre terá algum tipo de risco. O objetivo é que os tomadores de decisão devem sempre ter ciência dos riscos envolvidos tanto de não realizar o projeto quanto de sua realização.

Ressalta-se que Risco possuí uma relação inversamente proporcional a gestão destes riscos (maiores riscos assumidos equivalem a menores esforços na gestão de riscos).

6.3 Análise de Riscos

A análise de riscos visa identificar os riscos e ameaças e quais seus alcances no projeto, utilizando de métodos qualitativos e quantitativos. As ferramentas e técnicas usadas para identificação de riscos incluem, mas não se limitam:

- Entrevistas
- Brainstorming
- Análise de premissas de projeto
- Diagramas

Considerando a estrutura atual da área de TI, não será obrigatório documentar o processo de análise dos riscos, mas somente os riscos identificados.

6.4 Identificação de Incidentes

No documento interno de “Planos de Ação e Respostas a Incidentes”, deverá ser considerado todos os sistemas críticos da organização. Os incidentes aos sistemas de informação e dados podem ser, não se limitando, ocasionadas por:

- Acesso não autorizado;
- Ataques Cibernéticos;
- Falha no controle de temperatura e umidade;
- Falhas (hardware, software, mídia ou serviços de comunicação);
- Falta de pessoal;
- Manutenção/Procedimentos inadequados;
- Modificação acidental de dados (edição, remoção ou inclusão);
- Quedas de fornecimento de energia;
- Roubo;
- Sabotagem;
- Softwares maliciosos (malwares, vírus, worms, keyloggers, spywares, cavalos de troia, botwares ou denial-of-service).

Em caso de incidente que impacte os Clientes, estes devem ser informados da situação pela área responsável pelo processo impactado e qual o plano de ação definido para tratamento do incidente.

O incidente de segurança cibernética que afete processos críticos de negócios, ou dados ou informações sensíveis, e tenha impacto significativo sobre os clientes deve ser considerado relevante e comunicado a Superintendência de Relações com o Mercado e Intermediários (SMI).

Incidentes que possuem potencial de impactar processos críticos de negócios, ou dados ou informações sensíveis, e/ou tenha potencial de impactar os clientes também deve ser considerado relevante para criação de plano de ação.

6.5 Identificação de Vulnerabilidades

Vulnerabilidades são falhas nos procedimentos de segurança, de projeto, de implementação ou de controles internos que resultam (de forma acidental ou deliberada) numa brecha de segurança ou violação das políticas de segurança. As vulnerabilidades não estão unicamente ligadas a fatores tecnológicos, uma vez que podem estar atreladas ao comportamento do usuário, fatores sociais diversos ou políticas de autorização ou autenticação para controles de acesso.

A área de TI é responsável por identificar as vulnerabilidades por meio de fontes de divulgação de vulnerabilidades, verificações de vulnerabilidade ou realização de checklists de segurança.

Informações sobre vulnerabilidades podem ser coletadas em diversas fontes, incluindo verificações de vulnerabilidades realizados pela organização, relatórios de falhas, anomalias e testes de segurança realizados por empresas especializadas, divulgação por parte dos desenvolvedores de software (incluindo atualizações, hot fixes, patches, service packs, etc.,) e publicações da indústria de TI especializadas em vulnerabilidades.

Verificações contra falhas e vulnerabilidades devem fazer parte de uma rotina de verificação de segurança, conforme item “5.2.3 Avaliação de Ameaças e Vulnerabilidades”, visto que novas ameaças podem surgir com atualizações de hardware, software ou por descobertas e publicações de novas falhas.

Os checklists de segurança resultam do processo de comparação dos controles de segurança com os requisitos de segurança estipulados pela equipe de TI, contendo os padrões básicos de segurança para avaliação de possíveis vulnerabilidades.

Tanto a equipe própria da TI, quanto os seus fornecedores, devem se manter atualizados sobre os temas, inclusive com a participação de treinamentos, fóruns e leitura de relatórios acerca da segurança cibernética.

6.6 Monitoramento e revisão de riscos

O processo de Gerenciamento de Riscos deve estar atualizado e preciso, para tal o monitoramento e revisão deve ser uma parte planejada do processo de gerenciamento de riscos. Assim, todo o processo de gerenciamento de riscos, desde a verificação regular até os critérios de avaliação de risco usados também precisam ser revisados para garantir que eles permaneçam relevantes.

A busca pelo monitoramento automático deve ser uma busca constante, porém não elimina a necessidade de se realizar verificações manuais e ajustes nas rotinas.

7. ENGENHARIA SOCIAL

Engenharia Social é a habilidade de conseguir acesso a informações confidenciais através de habilidades de persuasão.

Para evitar esses problemas sempre verifique a origem dos e-mails e sua autenticidade e nunca instale softwares de origem maliciosa. Manter um programa de antivírus atualizado também é fundamental. Em caso de contatos telefônicos, sempre mantenha a calma e tenha plena certeza da origem e autenticidade da ligação.

Conhecer essas técnicas é de fundamental importância para a prevenção a informação, de forma que detalhamos abaixo algumas das informações, para os clientes e colaboradores se precaverem.

7.1 Phishing

É quando um cibercriminosos tenta enganar os usuários, através de envio de e-mails maliciosos, a fim de obter informações pessoais, sejam senhas, número de cartão de crédito, CPF, número de contas bancárias, etc. As abordagens dos e-mails de phishing podem ser as mais variadas tais como:

- Pela possibilidade de gerar para a vítima vantagem financeira, curiosidade ou despertar a caridade dela;
- Se passando pela comunicação oficial de Bancos, Lojas de comércio eletrônico, entre outros sites populares;
- Solicitando preenchimento de formulários com os seus dados pessoais;
- Instalando softwares maliciosos que possuem o objetivo de coletar informações sensíveis dos usuários;

Antes de clicar em um e-mail, é importante passar o mouse sobre o nome do remetente do e-mail para ver a real origem do e-mail. Nos casos dos e-mails enviados pela Amaril Franklin Corretora de Títulos e Valores Ltda, o remetente será sempre @amarilfranklin.com.br. Ressaltamos que a Amaril Franklin Corretora de Títulos e Valores Ltda nunca solicita informações de senhas, tokens, código de identificação do aparelho celular ou outros códigos de acesso.

7.2 Spam

Spam é o termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Os Spams são diretamente associados a ataques de segurança, através da propagação de códigos maliciosos, venda ilegal de produtos e disseminação de golpes.

7.3 Falso contato telefônico

Os fraudadores utilizam de técnicas para conseguir informações como dados pessoais, senhas, token, código de identificação do aparelho celular (IMEI) ou qualquer outro tipo de informação para a prática da fraude.

Ressaltamos que a Amaril Franklin Corretora de Títulos e Valores Ltda nunca solicita informações de senhas, tokens, código de identificação do aparelho celular ou outros códigos de acesso.

8. CONTINUIDADE DOS NEGÓCIOS

O processo de continuidade de negócios é implementado com o intuito de reduzir os impactos e perdas de ativos da informação após um incidente crítico a um nível aceitável, por meio do mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres.

A Amaril Franklin Corretora de Títulos e Valores Ltda mantém uma Política de Continuidade dos Negócios para tratar de forma específica este assunto.

9. ACESSO REMOTO DE COLABORADORES

O acesso remoto de colaboradores, para eventuais trabalhos na modalidade de Teletrabalho (Home Office), deverá ser avaliada e aprovada pela TI, sendo a liberação ou não do acesso registro suficiente dessa aprovação. O acesso só será permitido via VPN, conexão criptografada, considerando todas as regras de segurança descritos nessa política.

O controle de aprovação dos usuários será realizado pelo AD - Active Directory através do grupo de usuários específico para este fim. A área de TI poderá revogar o acesso dos usuários a qualquer momento a seu próprio critério.

10. CONTRATAÇÃO DE SERVIÇOS DE TERCEIROS DE TI

A Amaril Franklin Corretora de Títulos e Valores Ltda poderá realizar a contratação de Serviços de TI de Terceiros para o desenvolvimento de suas atividades diárias e para desenvolvimento de projetos específicos.

Para toda contratação de Serviços de Terceiros de TI, é necessário avaliar, gerenciar e monitorar o risco operacional decorrente do serviço contrato, que deverá ser realizado através do contato direto com o fornecedor por um colaborador da Amaril Franklin Corretora de Títulos e Valores Ltda que tenha interface direta com o fornecedor. O colaborador deverá reportar qualquer anormalidade a Diretoria de TI para que esta realize as devidas verificações.

10.1 Computação em Nuvem

A Amaril Franklin Corretora de Títulos e Valores Ltda deve se assegurar que o seu procedimento para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, atenda as regras previstas na Resolução 4.658/2018, do Banco Central do Brasil.

Todos os serviços contratos em nuvem devem atender a todos requisitos informados nessa política. Além disso, é preciso estabelecer métricas e indicadores adequados aos serviços contratados, assim como instituir o acompanhamento para identificação e correção de eventuais melhorias. Os procedimentos a serem seguidos no caso da interrupção dos serviços e o tratamento previsto para mitigar os efeitos dos incidentes, deve estar composto no “Plano de Ação e Respostas a Incidentes”, conforme item 5.2.8 dessa política.

10.2 Continuidade do Negócio em Nuvem

A Amaril Franklin Corretora de Títulos e Valores Ltda, conforme dito no item 8 – Continuidade de Negócios, possuí uma política específica de continuidade de negócios, porém no que tange a infraestrutura de TI utilizada, essa política é categórica ao colocar sobre a responsabilidade da área de TI a necessidade de planejar um possível reestabelecimento em caso de incidente relevante em nuvem.

Assim é importante que a área de TI possua mapeados potenciais fornecedores, para fornecer a estrutura em nuvem necessária, tenha em seus “Planos de Ação e Resposta a Incidentes”, conforme item 5.2.8 dessa política, planos que garantam a possiblidade de reestabelecimento já em nuvem, considerando as melhores práticas de mercado, tais como realização do Backup em Nuvem, virtualização de servidores, conexões de internet adequadas entre outras.

Neste caso, os cenários mais graves ficam relativos a falha dos servidores físicos atuais, sem tempo hábil para reposição de peças ou aquisição de novo servidor ou perda de toda estrutura física da Instituição (incêndio, desmoronamento ou condenação do prédio pelos órgãos competentes). Para tanto, o plano de reestabelecimento em nuvem deve considerar o prazo para reestabelecer o Backup já em nuvem permitindo o total funcionamento da corretora no menor tempo possível. Por fim, ao se contratar uma empresa para a prestação de serviço em nuvem é obrigatório mapear formas para se contratar outra empresa para substituição quando necessário.

O servidor em nuvem fornecido para guarda dos backups devem ser fornecido por um provedor diferente do servidor fornecido para o funcionamento das estruturas, ainda que disponibilizados pelo mesmo revendedor e deve ser realizado apenas por empresas que fornecem servidores dentro do Brasil e que garantem os padrões mínimos internacionais de segurança cibernética.

11. TRATAMENTO E CONTROLE DE DADOS DE CLIENTES

Todos os dados dos Clientes da Amaril Franklin Corretora de Títulos e Valores Ltda devem ser tratados como sensíveis, conforme já descrito no item 5.1 desta Política, dessa forma o acesso as informações de cadastro e de operações devem possuir controle de acesso que não permita a visualização, destruição, vazamento ou adulteração dos dados.

Sempre que possível, em especial aos sistemas com acesso externo, os dados que permitem a identificação devem ser criptografados diretamente nos banco, de modo que sem a quebra da criptografia os dados permaneçam anonimizados, ou seja, cuja identificação do proprietário não seja possível a partir das informações contidas na base dos sistemas.

Os dados solicitados aos clientes, servem para atendimento as normas e legislações vigentes dos órgãos reguladores do mercado financeiro, bem como realização de cadastro em outras instituições financeiras para a liberação de acesso aos produtos oferecidos. A Amaril Franklin Corretora de Títulos e Valores Ltda, ainda poderá utilizar-se desses dados para realizar análise de perfil de cliente, procedimentos de Prevenção a Lavagem de Dinheiro e Financiamento ao Terrorismo e realização de ofertas de produtos aderentes ao perfil do Cliente.

Os dados poderão ser compartilhados somente conforme casos descritos no Item “5.3 Confidencialidade e integridade da informação”.

12. ATRIBUIÇÕES BÁSICAS OU RESPONSABILIDADES ENVOLVIDAS

Quaisquer indícios de irregularidades no cumprimento das determinações desta Política serão alvo de investigação interna e devem ser comunicadas imediatamente aos nossos canais de atendimento.

12.1 Usuários/colaboradores

Todos os colaboradores devem ter ciência das normas, procedimentos, orientações e outras informações relevantes acerca de segurança que permitam a execução de suas atribuições sem comprometer a segurança.

Os usuários deverão notificar imediatamente o setor de TI acerca de qualquer fragilidade, risco, ameaça ou quebra de segurança detectada ou suspeita. Em nenhuma circunstância, o colaborador deve investigar a notificação.

12.2 Da Tecnologia da Informação

Ficará responsável pela monitoração da aplicação dos parâmetros e limites de normalidade operacional, documentando exceções e eventos susceptíveis de relatos e procedimentos de medida preventiva.

Garantir que sistemas, processos e infraestrutura de TI sejam robustos e adequados às necessidades e às mudanças do modelo de negócio, tanto em circunstâncias normais quanto em períodos de estresse.

Na ocorrência de algum fato que contrarie o determinado neste documento, a área de TI regularizará imediatamente a situação, relatando o problema e a solução adotada ao Diretor da área, através do formulário **REGISTRO DE OCORRÊNCIA**, conforme estabelecido na matéria – **MONITORAÇÃO E SOLUÇÃO DE PROBLEMAS** do Manual de Controles Internos da Amaril Franklin Corretora de Títulos e Valores Ltda.

12.3 Da Diretoria

É responsável pela aprovação da Política de Segurança da Informação, do acompanhamento do desenvolvimento das ações nos ajustes necessários para adequação dos procedimentos. Além disso deve manter o comprometimento com a melhoria contínua dos procedimentos relacionados com a segurança cibernética.

Belo Horizonte, Revisado em 04/04/2023

AMARIL FRANKLIN CORRETORA DE TITULOS E VALORES LTDA