




Política de Tecnologia da Informação

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

Sumário

1. Apresentação	3
2. Objetivo	3
3. Políticas de Tecnologia da Informação	3
3.1. Acesso ao Ambiente Operacional e Sistemas	3
3.2. Segurança da Informação e Cibernética	7
3.2.1. Atribuições e Responsabilidades	8
3.2.2. Principais Características	9
3.2.3. Segurança e Uso Responsável de Recursos de TI	11
3.3. Política de Gestão de Incidentes	24
3.4. Contingência Operacional	32
3.4.1. Geral	32
3.5. Política de Privacidade de Dados	33
3.6. Política de Gestão de Acessos	40
3.7. Política de Gestão de Backups	45
3.8. Política de Cookies	47
3.9. Política de Gestão de Ativos	49

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

1. Apresentação

É fundamental ressaltar que o presente documento é divulgado de forma transparente e acessível a todos os funcionários, parceiros e prestadores de serviços terceirizados. Comprometemo-nos a manter esta política atualizada e a assegurar sua aplicação em todas as unidades da instituição, inclusive aquelas situadas no exterior.

O Departamento de Compliance é designado como responsável por toda e qualquer alteração, atualização e divulgação do presente material. As manutenções são realizadas por meio de um conjunto de regras próprias, com envolvimento das áreas afins, garantindo assim a eficácia e relevância contínua da nossa abordagem de prevenção à lavagem de dinheiro e ao financiamento do terrorismo.

2. Objetivo

Esta Política tem como objetivo estabelecer as diretrizes mais importantes para minimizar os riscos dos negócios, disciplinando a ação gerencial, mantendo a ordem administrativa e fundamentando a eficácia dos processos operacionais.

Esta Política contém informações indispensáveis para o corpo diretivo e gerencial da **Freex Corretora de Câmbio S/A**.


3. Políticas de Tecnologia da Informação

3.1. Acesso ao Ambiente Operacional e Sistemas

Garantir a segurança na concessão de acessos ao ambiente operacional e sistemas da Freex Corretora de Câmbio.

Solicitação de Acessos / Bloqueios Sistêmicos

Os pedidos de acesso/bloqueio devem ser feitos através de chamado, para então ficarem documentados para posterior auditoria.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

Movimentação de Funcionários

A Área de Recursos Humanos é responsável pela informação da movimentação de Funcionários:

- Contratação;
- Troca de área / função;
- Desligamento.

Nota: Necessidades de acesso à novo sistema / transação deverá ser solicitadas pelo Gestor do funcionário.

Movimentação de Colaboradores - PJ

As Áreas são responsáveis pela informação da movimentação de seus respectivos colaboradores:

- Contratação;
- Troca de área / função;
- Acesso novo sistema / transação;
- Desligamento.

Cadastramento de Acessos / Bloqueios Sistêmicos

É de responsabilidade do **Departamento de Tecnologia da Informação**:

Movimentação de Funcionários / colaboradores – PJ:

Contratação


Cadastramento de “usuário” e “login” de acesso à rede e disponibilização de “e-mail”.

Regra para nomenclatura de usuário: Primeira letra do nome, mais o último sobrenome. Caso a nomenclatura já exista, o critério será: primeira letra do nome, mais a primeira letra do primeiro sobrenome, mais o último sobrenome.

É utilizado o AD (Active Directory) da Microsoft que é do Windows Server.

Desligamento

Desabilitação de acessos.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

- Manter atualizada “Planilha de Controle” (própria) de Funcionários / colaboradores - PJ, realizando periodicamente revisões e manutenções (a cada 30 dias).

É de responsabilidade do **Departamento de Tecnologia da Informação**:

Movimentação de Funcionários / colaboradores – PJ:

Contratação

Cadastramento de “perfil” de acesso aos sistemas.

Troca de área/função

Alteração do “perfil” de acesso aos sistemas.

Acesso à novo sistema / transação

Liberação de acesso ao sistema/transação.

Desligamento

Desabilitação de acesso aos sistemas.

- Manter atualizada “Planilha de Controle” (própria) de Funcionários / colaboradores - PJ por sistema e perfil, realizando periodicamente revisões e manutenções (a cada 30 dias).
- Efetuar a gestão / manutenção (inclusão, exclusão, transferência) de visibilidade da Área Comercial à base de clientes, conforme solicitação dos respectivos gestores responsáveis.
- Fornece às Áreas de Operações e Presidência, no primeiro dia útil de cada mês, relação atualizada dos colaboradores – PJ.


Senhas “Administrador, Master ou root” – Sistemas / Rede

As senhas “Administrador, master ou root” de acesso aos sistemas e à rede são devidamente registradas (criptografadas) através de software específico e mantidas sob o controle do Departamento de Tecnologia da Informação.

Senhas dos Usuários

As senhas são de uso pessoal e intransferível. Deverão ser substituídas periodicamente (mensal) ou a qualquer tempo, conforme necessidade.

Geração de Senhas para Redes Locais e Sistemas

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

A geração de senhas obedecerá aos critérios a seguir, considerando a flexibilidade dos respectivos softwares:

As senhas devem obedecer às regras de complexidade na seguinte condição:

- Possuir caracteres alfanuméricos, maiúsculos e minúsculos;
- Possuir pelo menos um caractere Maiúsculo mais um caractere alfabético e um especial.

As senhas devem obedecer à regra de não repetição das 5 (dez) últimas senhas.

As senhas devem possuir, no mínimo, 8 (seis) caracteres alfanuméricos observados no item “regras de complexidade”.

O prazo para vencimento das senhas deve ser de, no MÁXIMO, 90 dias.

O vencimento das senhas deve ser automático devendo o software requisitar a troca de senha do usuário assim que ela estiver para vencer.

As senhas devem ser configuradas de forma que, após 5 (cinco) tentativas fracassadas de acesso, o usuário estará BLOQUEADO para uso:

- Para liberação do acesso após bloqueio, deve ser formalizado à área de segurança de informações, o pedido de desbloqueio com ciência da estrutura do solicitante.
- Em sendo um usuário interno de sistemas e com ocorrência de Bloqueio, deve ser instaurado processo investigativo técnico pela área de segurança de informações. Para este caso o desbloqueio deve ser efetuado conforme interpretação da área de segurança de informações.


As senhas de usuários GENÉRICOS ou de SISTEMAS INTERNOS deverão ser criptografadas e registradas em software.

Geração de Senhas para Bancos de Dados

A geração de senhas obedecerá aos critérios a seguir:

As senhas de bancos de dados devem obedecer às regras de complexidade:

- Possuir caracteres alfanuméricos, maiúsculos e minúsculos;

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

- Possuir pelo menos um caractere Maiúsculo mais um caractere alfabético e um especial.

As senhas de bancos de dados devem obedecer à regra de não repetição das 10 últimas senhas.

As senhas de bancos de dados devem possuir, no mínimo, 6 caracteres alfanuméricos observados no item “regras de complexidade”.

O vencimento das senhas será coordenado por solicitação da Superintendência ou por motivos de força maior.

As senhas de bancos de dados deverão ser criptografadas para uso pelos aplicativos contratados (aplicações devem possuir formato de geração de criptografia de senha – hash – o qual será gerado em arquivos para acesso pela aplicação).


Verificação de Usuários/Acessos

É atribuição do Departamento de Tecnologia da Informação para cada sistema/módulo a validação mensal dos usuários e perfis cadastrados nos respectivos sistemas.

3.2. Segurança da Informação e Cibernética

Os objetivos desta política são:

- Compreender a necessidade de sigilo sob quaisquer informações que se possua acesso para execução de seu trabalho, desta forma mantendo os dados/informações e estratégias da Corretora somente dentro do grupo organizacional, não fornecendo a terceiros, salvo com existência de autorização expressa da Presidência da Corretora.
- Delinear a forma de uso aceitável dos equipamentos, softwares e sistemas de informação da Freex Corretora de Câmbio. As orientações e regras aqui contidas são estabelecidas para prover meios de proteção tanto os Funcionários, clientes, parceiros, especialistas, Funcionários contratados em regime temporário, incluindo pessoal integrante de empresas contratadas, de ameaças, incluindo ataques de vírus, comprometimento da rede e dos serviços e assim como de questões legais.
- Orientar sobre o uso, armazenagem e destruição de documentos contendo informações confidenciais, sejam relativas aos clientes, sejam relativas aos negócios da contratante, bem como os riscos associados ao uso e destruição inadequada deles.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

3.2.1. Atribuições e Responsabilidades

Diretoria Administrativa Financeira

- Deliberar sobre normas internas de segurança da informação;
- Respaldar financeiramente projetos de melhoria da segurança da informação e cibernética da Corretora.

DPO - Data Protection Officer


- Orientar os funcionários e os contratados da Freex Corretora de Câmbio a respeito das práticas a serem tomadas em relação à proteção de dados pessoais de Clientes.
- Comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular dos dados pessoais a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante a esses dados.

Gestor de Risco

- Analisar casos de violação da segurança da informação, acompanhando as providências imediatas pelo responsável pelo tratamento de dados pessoais;
- Garantir a divulgação da política de segurança da informação, bem como das normas e procedimentos vinculados a esta política;
- Analisar e mitigar os riscos relacionados à segurança da informação;
- Requisitar informações das demais áreas, com o intuito de verificar o cumprimento da Política e das Normas da segurança da informação;
- Obter as informações necessárias para a elaboração do Relatório de Impacto à Proteção de Dados Pessoais.

Responsabilidades Gerais

- Todas as informações trocadas ou armazenadas na Freex Corretora de Câmbio, independentemente de conteúdo, são de propriedade única e exclusiva da Corretora. Os usuários devem utilizar os recursos disponibilizados pela Corretora apenas para a condução dos seus negócios;
- Compete a todos os Colaboradores o cumprimento das diretrizes constantes desta Política e das demais diretrizes de Segurança da Informação e Cibernética;
- Todo colaborador deve aderir, formalmente, ao Contrato/Termo de Segurança;

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

- Devem informar imediatamente, à Área de Gestão de Riscos todas as violações às políticas de segurança da informação, incidentes, violações de acessos ou anomalias que possam indicar a possibilidade de incidentes, sobre os quais venham a tomar conhecimento.

3.2.2. Principais Características


A Estrutura normativa da Segurança da Informação da Freex Corretora de Câmbio é composta por um conjunto de documentos com níveis hierárquicos distintos, relacionados a seguir:

- Política de Segurança da Informação: define estrutura, diretrizes e as obrigações referentes a segurança da informação;
- Normas de Segurança da Informação: estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos em diversas situações em que a informação é tratada;
- Procedimentos de Segurança da Informação: instrumentalizam o disposto nas Normas e na Política, permitindo a direta aplicação nas atividades da Corretora.

A Freex Corretora de Câmbio tem seus processos de Segurança de Informação controlados pelas atividades a seguir, através de seus responsáveis:

Organização da Segurança da Informação

- A Presidência deve apoiar ativamente a Segurança da Informação da Corretora;
- A coordenação das atividades de segurança da informação deve ser realizada pelo Gestor de Segurança da Informação em conjunto com representantes de diferentes áreas estratégicas da Instituição;
- As responsabilidades pela segurança da informação devem estar claramente definidas e divulgadas, inclusive nos casos de terceiros, parceiros e fornecedores;
- As políticas e procedimentos de segurança devem ser revisados e atualizados sempre que houver um fato relevante decorrente de nova legislação ou de nova estratégia da Instituição, considerando todos os fatos e eventos relevantes que exijam, inclusive, revisão imediata.


	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

Segurança na Contratação dos Recursos Humanos

- Assegurar que colaboradores, fornecedores e terceiros entendam seus papéis e responsabilidades, antes, durante e no encerramento ou mudança da contratação, visando reduzir o risco de roubo, fraude e mal uso de recursos;
- Assegurar que todos os candidatos a emprego sejam adequadamente analisados, especialmente em cargos ou serviços com acesso a informações confidenciais. São obrigatórias as verificações de referências pessoais;
- Garantir que todos os novos colaboradores e terceiros recebam instruções sobre sua responsabilidade pela segurança da informação e que todos assinem um Contrato de Segurança;
- Estabelecer planos de treinamento e conscientização periódicos, garantindo a ciência e aderência dos colaboradores e terceiros e diretrizes da segurança da informação;
- Garantir a devolução dos ativos da Freex Corretora de Câmbio e a retirada de direitos de acesso de todos os colaboradores, terceiros e fornecedores no encerramento de suas atividades, contratos ou acordos;
- Aplicar as medidas disciplinares formais vigentes para os colaboradores que tenham cometido violação de Segurança da Informação garantindo, inclusive, dissuasão para que novas violações ocorram.

Gestão das Operações e Comunicações

- Garantir a operação segura e correta dos recursos de informação da Freex Corretora de Câmbio, incluindo as atividades de rede, bem como o controle e detecção de atividades não autorizadas;
- Assegurar que os procedimentos de operação sejam documentados, mantidos atualizados e disponíveis a todos os usuários que deles necessitem;
- Monitorar a utilização dos recursos e realizar projeções para necessidades futuras, garantindo o desempenho requerido do sistema;
- Implantar controles de detecção, prevenção e recuperação para proteção contra códigos maliciosos e intrusões;
- Realizar e testar regularmente as cópias de segurança das informações e softwares (backups) e armazenar em local físico diferente e distante da localidade dos dados originais;
- Descartar de forma segura e protegida as mídias e equipamentos, quando não forem mais necessários, observando-se a classificação das informações armazenadas;

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

- Realizar de forma a não permitir “acesso não autorizado”, uso impróprio ou alteração indevida, o transporte externo de mídias e documentos. Mídias com informações “CONFIDENCIAIS” devem ter seus conteúdos criptografados antes do transporte externo;
- Garantir a aderência aos controles de uso da Internet e de Correio Eletrônico (e-mails), definidos em políticas específicas.

3.2.3. Segurança e Uso Responsável de Recursos de TI

Apresenta as normativas de uso dos ativos de Tecnologia de Informação da Freex Corretora de Câmbio, visando à preservação da Segurança de Informações e da integridade deles.


Esta política fornece orientação e regras para a promoção do uso adequado e responsável dos recursos de Tecnologia da Informação (TI) da Freex Corretora de Câmbio, com o intuito de prover meios para proteger nossos usuários e a própria Corretora de ações ilegais ou danos que possam ser perpetradas por pessoas, internas ou externas, sejam estas ações intencionais ou acidentais.

Definições

No decorrer deste documento utilizaremos alguns termos técnicos e expressões que podem não ser de conhecimento imediato dos usuários.

Consideram-se como recursos de TI (Tecnologia da Informação) qualquer item considerado, mas não limitado, as descrições abaixo:

Hardware	Conjunto de componentes físicos de um equipamento com capacidade de processamento de informações.
Microcomputador	Equipamento de pequeno porte utilizado para execução de programas. Geralmente dedicado a um usuário ordinário.
Servidor	Equipamento central de média ou grande capacidade de processamento dedicado ao processamento de informações corporativas.
Roteadores	Equipamento especializado para controle de redes locais.
Switches	Equipamento especializado para controle de redes locais.
Hubs	Equipamento especializado para controle de redes locais.
Firewalls	Equipamento dedicado a funções de segurança de rede.
Pendrives	Dispositivos móveis para armazenamento de informações.
DVD, Blu Ray (R/RW)	Dispositivos móveis para armazenamento de informações.


	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

Nuvem	Armazena dados na Internet por meio de um provedor de computação na nuvem.
Mídias de armazenamento	Dispositivos dedicados ao armazenamento de informações. Ex. fitas magnéticas, pendrives, disquetes.
Software	Programa ou conjunto de programas de um computador.
E-mail	Programa de Correio eletrônico.
Internet	Rede mundial de Informações em computadores.
Intranet	Rede interna de Informações residentes em computadores.
Contas de Rede	Credencial de usuário concedida pela área de TI.
Browser	Programa especializado para acesso a informações da Internet ou Intranet.
Telefones Digitais	Equipamentos de telefonia digital.
Telefones Analógicos	Equipamentos de telefonia convencional.
PABX	Central Telefônica Corporativa.
Links de comunicação	Canais de comunicação entre pontos remotos (ex.: agências).
Impressoras	Equipamentos destinados à impressão de informações existentes em computadores.
Tablet	Computadores portáteis de mão.
Notebooks	Computadores portáteis.
Rede Local	Conjunto de computadores interligados.

Uso geral de recursos de TI

Os recursos de TI da rede, incluindo, mas não limitado a microcomputadores, servidores, equipamentos de segurança (firewalls), equipamentos de controle de rede local (roteadores, switches, hubs), softwares, sistemas operacionais, mídias de armazenamento, contas na rede, e-mail, acesso à Internet e Intranet, devem ser utilizados estritamente para fins a que se destina no interesse da Freex Corretora de Câmbio.

- Os usuários dos recursos de TI, são responsáveis pela utilização correta destes colocados à sua disposição, e das informações neles disponibilizadas.
- As empresas que possuam profissionais alocados nas dependências da Corretora e que venham a ser usuários dos recursos de TI devem prover orientações, aos mesmos, sobre o uso responsável dos recursos e das informações disponibilizadas pela Freex Corretora de Câmbio.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024


Mecanismos de proteção dos recursos de TI

A Freex Corretora de Câmbio considera como imprescindível o direito de proteger seus ativos de TI, desde equipamentos, softwares até as informações tendo implantado as seguintes ferramentas e políticas:

- Os microcomputadores não possuem unidades CD (ROM ou RW), DVD (ROM ou RW), portas USB habilitadas (fora do uso permitido).
- O acesso à rede local para um novo usuário é concedido após processo conjunto de avaliação junto às áreas de Recursos Humanos e gestoras de negócios.
- Possuímos políticas de concessão de direitos de acesso a informações das áreas de negócio sendo de responsabilidade do gestor de cada área, autorizar a concessão do acesso.
- O acesso à Internet e correio eletrônico é monitorado por ferramentas de mercado sendo de direito da Corretora, a avaliação do conteúdo das mensagens trafegadas na rede.
- Necessidades eventuais ou regulares de envio ou recebimento de informações em mídias removíveis deverão ser tratadas junto à Presidência.
- A liberação de acesso extraordinária a sites na Internet é efetuada a partir de autorização da área de Segurança de Informações por escrito (e-mail, documentação), a partir de solicitação igualmente documentada.
- As fronteiras entre os recursos de TI e o meio externo (Internet, conexão com outras empresas) são controladas e monitoradas por equipamentos de segurança (Firewalls, IDS etc.).
- Estão instalados, nos computadores da Freex Corretora de Câmbio, sistemas de detecção e combate a vírus e programas maliciosos (tem como finalidade a exploração de informações confidenciais), com atualização automática contra novas ameaças.
- As configurações do sistema operacional residente nos computadores da Corretora, fornecem acesso limitado aos recursos dos equipamentos.
- Usuários em período de férias ou afastados de suas atividades tem suas credenciais de acesso bloqueados durante o período de afastamento.

Condições de uso dos recursos de TI

As seguintes condições são consideradas como não autorizadas:

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

Violação de propriedade Intelectual


- Utilizar ou divulgar material que viole direitos de propriedade intelectual de qualquer pessoa ou companhia, como marca registrada, nome comercial, segredo empresarial, domínio na internet, patentes, desenho industrial ou qualquer outro material, não autorizado expressamente pelo autor, que viole direito de propriedade industrial, artística ou literária;
- Instalar, distribuir ou utilizar softwares “pirateados” ou não licenciados para uso na Freex Corretora de Câmbio;
- Fazer cópia não autorizada de material protegido por direitos autorais, incluindo, mas não limitado a: músicas, textos, digitalização e distribuição de fotografias encontradas em revistas, livros ou em outras fontes protegidas por direitos autorais.

Manipulação não autorizada de informações e programas de computador

- Criar, transmitir, distribuir, colocar, armazenar ou tornar disponível através da Corretora e da Internet qualquer material que viole leis ou regulamentações referentes à obscenidade, pornografia ou pedofilia;
- Utilizar material que divulgue informações injuriosas, caluniosas ou difamatórias, que viole o direito à honra ou à imagem das pessoas. Material que constitua ameaça a alguém ou qualquer material que viole quaisquer leis e regulamentações vigentes;
- Divulgar informações confidenciais ou classificadas como estratégicas para a Corretora sob qualquer forma (e-mail, cópias, impressão, etc.);
- Introduzir programas com códigos maliciosos na rede ou servidores (exemplo: vírus, worms-vermes, cavalos de Tróia, phishing);
- Divulgar informações de clientes, produtos, Funcionários, empresas contratadas, colaboradores e parceiros sem prévia autorização da Presidência da Freex Corretora de Câmbio.

Uso indevido de credenciais e senhas de acesso

- Divulgar códigos de identificação, autenticação e autorização de uso pessoal (conta de rede, senhas) ou permitir o uso por terceiros de recursos autorizados por meio desses códigos;
- Fornecer informações a terceiros sobre Funcionários ou lista de Funcionários de entidades usuárias da Freex Corretora de Câmbio, sem autorização expressa;

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

- Tentar se utilizar de engenharia social (relacionamentos pessoais, abuso de autoridade, confiança) para obtenção de informações confidenciais ou credenciais de acesso a sistemas e infraestrutura.

Violação de equipamentos

- Instalar ou tentar instalar nos computadores de propriedade da Freex Corretora de Câmbio, unidades de mídia de armazenamento tais como, mas não limitados a: pendrives, discos rígidos, cartões de memória, ou quaisquer outros dispositivos de armazenamento interno ou externo;
- Conectar ou tentar conectar, alguma forma de equipamento portátil tal como: Palmtops (computadores de mão), Notebooks e Laptops na rede local da Corretora.

Equipamentos

- Utilizar equipamentos pessoais (Notebooks) nas dependências da Corretora, quer seja para desenvolvimento das funções profissionais ou para fins pessoais.

As exceções serão tratadas na esfera da Presidência devendo ser devidamente documentadas.

Acesso indevido à internet e ao correio eletrônico


As seguintes condições são consideradas como não autorizadas:

Uso da Internet

Acessar sites (sítios) na Internet cujo conteúdo esteja classificado, mas não limitado, dentro das alternativas abaixo descritas as quais são consideradas como impróprias para as suas funções na Freex Corretora de Câmbio.

Conteúdos classificados como impróprios para acesso:

- Erótico ou pornográfico (de qualquer tipo).
- Racismo e discriminação.
- Militância política.
- Ocultismo.
- Difamação de entidades públicas ou privadas.
- Esportes, apostas on-line.
- Jogos on-line.
- Conversação pela internet (Chats, Mensageiros, etc.).

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

- WEB Mail (correio eletrônico em páginas na internet).
- Grupos de relacionamento e redes sociais (FaceBook e assemelhados).
- Relacionados à prática ou estudo de formas de ataque aos ativos de TI quer seja com objetivos de ganho financeiro ou não.

Correio eletrônico (E-mail) Interno e Externo (internet)

Utilizar recursos de e-mail para envio de mensagens com conteúdo classificado como indevido ou não ético (pedofilia, pornografia, escárnio, ofensas aos bons costumes locais, cunho difamatório de qualquer espécie, correntes, apostas, entre outros).

Utilizar programas de newsgroup (comunidades, mensagens instantâneas), nas instalações da Freex Corretora de Câmbio.


Utilizar recursos de TI da Corretora para tráfego de mensagens instantâneas, comunidades virtuais na Internet ou na intranet que não estejam diretamente relacionadas com o seu negócio e sem a prévia autorização das estruturas da área.

Utilizar recursos de TI da Corretora para repassar, internamente ou externamente, mensagens com conteúdo inadequado para a condução normal das atividades do usuário (piadas, diversão, pornografia, esporte, escárnio).

Acesso indevido à rede de dados

As seguintes condições são consideradas como não autorizadas:

- Obter acesso não autorizado a dados, sistemas, redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades da rede, dispositivos da rede, ou violar a segurança ou medidas de autenticação, sem autorização expressa da Presidência da Freex Corretora de Câmbio.
- Efetuar monitoração não autorizada de dados ou tráfego em qualquer rede, sem a autorização expressa Presidência da Corretora.
- Executar qualquer forma de monitoramento da rede o qual interceptará dados não destinados ao endereço do equipamento do usuário, a menos que essa atividade seja parte do trabalho normal do funcionário com a aprovação da Presidência da Corretora.
- Fazer tentativas deliberadas para interferir em um serviço, sobrecarregar um serviço ou, ainda, tentar desativar um servidor, inclusive aderir a ataques de negação de serviços quer seja para obter qualquer ganho como para testar a segurança da Corretora.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

- Utilizar comandos, batches, programas, scripts ou enviar mensagens de qualquer espécie com a intenção de interferir ou desabilitar uma sessão de usuário, via qualquer meio, localmente ou remoto.
- Obter acesso aos recursos da rede de informações (servidor, rede, conta de correio, sistemas aplicativos) sem a devida autenticação, através de meios fraudulentos.

Reprodução não autorizada de imagem e voz

- Efetuar qualquer tipo de reprodução de imagem (câmeras fotográficas, câmeras embutidas em celulares) em qualquer meio digital ou analógico dentro das dependências da Freex Corretora de Câmbio sem prévia autorização.
- Utilizar qualquer recurso para reprodução de voz (gravadores, escutas telefônicas, captura de voz) em qualquer meio digital ou analógico dentro das dependências da Corretora.

Exceções

Usuários da área de Tecnologia da Informação na execução de suas responsabilidades poderão estar isentos dessas restrições (administradores de redes) desde que previamente autorizados pela Presidência estarão autorizados a interferir nos acessos de equipamentos se este estiver afetando negativamente os serviços da Freex Corretora de Câmbio.


As exceções serão tratadas na esfera da Presidência devendo ser devidamente documentadas.

Monitoramento de ocorrências e controles adicionais

A Freex Corretora de Câmbio reserva-se o direito de gravar as ligações de seus Funcionários e colaboradores através de seus ramais telefônicos. Da mesma forma, são gravadas cópias das mensagens enviadas ou recebidas pelos Funcionários através do sistema de correio eletrônico (e-mail).

O objetivo destas gravações é primordialmente fornecer subsídios para esclarecer dúvidas relativas a operações que tenham sido realizadas por telefone ou tenham tido detalhes informados via e-mail. Entretanto a Corretora reserva-se o direito de analisar o conteúdo destas gravações sempre que julgar necessário, com o intuito de assegurar-se da não transmissão de informações classificadas como confidenciais ou estratégicas.

A divulgação de dados confidenciais ou estratégicos para terceiros ou estranhos às atividades funcionais, através de e-mail ou telefone é uma violação do Código de Ética da Freex


	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

Corretora de Câmbio, caracterizando-se como falta grave, sujeitando-se as pessoas envolvidas às sanções decididas pela Presidência.

Recomendações importantes

Abaixo seguem algumas recomendações importantes para manter a segurança das informações da Corretora:

- Nunca discutir informações estratégicas em locais de circulação pública tais como: elevadores, corredores, e áreas comuns da Corretora.
- Não deixar impressões de informações estratégicas em locais inadequados (impressora, mesas, armários sem chave).
- Não deixar nenhum material com informações pertinentes à Corretora, exposto em mesas, impressoras, scanners e outros lugares.
- Destruir por completo materiais com informações classificadas como confidenciais (estratégicas para os negócios da Corretora) e que tenham de ser descartados. Podem-se aproveitar os picotadores de papel existentes ou destruí-los manualmente.
- Não jogar mídias de armazenamento de informações no lixo sem antes destruí-las por completo.
- Não efetuar mudanças de layout de recursos de TI; sempre acionar a Diretoria Executiva para tal.
- Não abrir nenhum e-mail que não se conheça a origem (remetentes não identificados ou suspeitos), que não declare o assunto ou que não possua relação com o trabalho do usuário.
- Nunca executar programas ou tentar abrir imagens, vídeos, filmes ou qualquer outro conteúdo enviado por e-mail às caixas postais do usuário.
- Nunca fornecer credenciais de acesso ou informações de contas bancárias e senhas, ou dados pessoais (inclusive documentação) por e-mail, em sites na internet ou ainda por telefone sem ter absoluta certeza da idoneidade do solicitante da informação.
- Avisar à Presidência em casos de recebimento contínuo ou esporádico de e-mails onde não se conheça a origem ou com assunto estranho ao trabalho do usuário.
- Sempre dar ciência ao gestor da área ou às Diretorias sobre ocorrências de violações da política de segurança perpetradas por quem quer que seja. As informações prestadas serão tratadas com confidencialidade.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

Ações de controle contra violações da política e medidas disciplinares.

Caso ocorram violações a esta política, a Freex Corretora de Câmbio reserva-se ao direito de adotar as medidas disciplinares que sejam cabíveis para o caso.

Os casos de violação terão as medidas disciplinares tratadas no nível da Presidência e diretorias da Corretora.

O conhecimento de uma violação desta política por parte de Funcionários ou prestadores de serviço e não informada aos gestores ou à Presidência, constitui falta grave passível das mesmas medidas disciplinares a serem tomadas contra o infrator.

A Presidência investigará os incidentes de segurança detectados e poderá se envolver e cooperar na aplicação da lei no caso de haver suspeita de violação que se caracterize como crime.

Segurança de Documentos


Tem como objetivo disciplinar o uso da informação dentro da Freex Corretora de Câmbio, preservando o sigilo dos clientes e de informações internas consideradas como estratégicas.

Introdução

Todas as instituições Financeiras autorizadas, tem o dever de zelar pelo sigilo dos dados apresentados por seus clientes. Esta obrigação está regulamentada através da Lei Complementar 105/2001, que define como risco operacional a possibilidade de ocorrência de perdas resultantes de falhas na proteção e na segurança de dados sensíveis relacionados tanto às credenciais dos usuários finais quanto a outras informações trocadas com o objetivo de efetuar transações de pagamento.

Assim, o presente documento apresenta orientações sobre como classificar um documento, em função da informação nele registrada, além de orientações sobre a custódia desta informação e meios a serem utilizados para destruição de informações classificadas como confidenciais.

Parte das informações aqui apresentadas encontra-se registrada no Código de Ética, disponibilizado a todos os Funcionários.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

Classificação de Informações

Toda informação pode ser classificada em níveis de confidencialidade, dependendo da importância da informação e dos riscos associados a uma eventual divulgação indevida. Abaixo segue uma recomendação para a classificação do grau de confidencialidade das informações.

Não classificadas – Informações de uso geral, que não comprometam a Corretora e possam ser divulgadas internamente sem preocupações.

Uso Interno – Informações cuja divulgação possa ser inconveniente ou inapropriada, pois tratam de assuntos exclusivamente internos.

Divulgação Restrita – A divulgação destas informações pode causar problemas ou prejuízos à Freex Corretora de Câmbio.

O acesso e o tratamento da informação de acesso restrito ficam limitados às pessoas que tenham necessidade de conhecê-la.

Confidencial – Informações cuja divulgação possam causar sérios problemas. Todas as informações relativas a clientes são classificadas como confidenciais.

O uso do bom senso é fundamental para avaliar o grau de confidencialidade das informações, entretanto os Funcionários devem discutir o assunto com seus gestores sempre que surgirem dúvidas, antes de qualquer divulgação.


Utilização de Informações

É vedada a divulgação externa de informações, classificadas como confidenciais recebidas pelos Funcionários da Freex Corretora de Câmbio, devendo obedecer estritamente às instruções de manuseio.

É importante lembrar que o funcionário da Corretora tem acesso a dados reservados dos clientes, tais como, Informações pessoais do cliente (Endereço, renda, empresa onde trabalha etc.).

Estas informações são protegidas por lei e, portanto, devem ser tratadas com o rigor e cuidado necessário.

O descuido no tratamento destas informações poderá acarretar ao infrator, medidas punitivas classificadas no código civil e bancário brasileiro.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

Proteção de Informações


Com o intuito de proteger a Freex Corretora de Câmbio e seus clientes de eventuais vazamentos de informações, as seguintes orientações devem ser cumpridas por todos os Funcionários da Corretora:

- Nunca imprimir um documento que contenha informações sobre o cliente ou informações confidenciais da Corretora se não houver uma real necessidade;
- Caso a impressão deste documento seja realmente imprescindível, o mesmo deverá ser arquivado em pastas e mantido em arquivos fechados/trancados;
- Caso o documento não seja mais necessário, a informação impressa deverá ser destruída imediatamente;
- Os documentos impressos devem ser retirados das impressoras imediatamente, evitando o acesso de outros Funcionários aos mesmos;
- Todos os relatórios e outros documentos que não forem arquivados devem ser encaminhados para destruição;
- Cópias de documentos devem ser tratadas com o mesmo rigor que os documentos originais, ou seja, destinadas a um arquivo fechado ou a destruição.
- Documentos apresentados por clientes (comprovante de residência, comprovante de rendimentos, documentos pessoais) que não sejam utilizados para a adesão ao produto devem ser encaminhados para destruição;
- Documentos ou cópias de documentos não devem ser jogados em cestos de lixo comum em hipótese alguma. Os mesmos devem ser fragmentados e descartados;
- Os armários onde são arquivados documentos confidenciais devem ser mantidos trancados durante todo o tempo;
- As gavetas de mesas devem ser mantidas fechadas à chave.

Mesas Limpas

Esta política refere-se à Mesa, Tela, Impressora e Lixo Limpos:

- Ao se ausentar, o colaborador não deve deixar sobre a mesa de trabalho impressos, anotações, agendas e cadernos. Estes devem ser guardados em gavetas ou armários com trancas;
- A utilização de proteção de tela, com senha, em computadores é responsabilidade obrigatória do colaborador. Apesar da proteção de tela ser acionada automaticamente em

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

períodos de inatividade do mouse ou teclado, o usuário deve acioná-la, imediatamente, antes de sua ausência da mesa de trabalho;

- É imperativo manter documentos impressos e dispositivos de armazenamento devidamente protegidos, não deixando estes materiais na impressora ou na lixeira. Devem ser guardados em armários com chaves, descartados em lixos protegidos ou devem ser triturados.
- Documentos soltos sobre a mesa de trabalho podem ser extraviados facilmente, ter suas informações acessadas por outras pessoas, além de agirem como propagador de chamas na eventualidade de um incêndio;
- Não deve ser deixado sobre a mesa de trabalho nenhum documento confidencial que não seja utilizado imediatamente.

Deve ser implantado processo de monitoramento das ocorrências desta política para conscientização e reorientação.

A Freex Corretora de Câmbio determina que informações não divulgadas publicamente devam ser protegidas adequadamente, visando o cumprimento da legislação e regulamentação aplicáveis.

Ações de controle contra violações da política e medidas disciplinares


As ações contra violações da política e medidas disciplinares a serem aplicadas são as mesmas descritas no item “Segurança e Uso Responsável de Recursos de TI”.

Segurança Cibernética

A política de Segurança Cibernética da Freex Corretora de Câmbio tem como visão garantir a proteção, a manutenção da privacidade, integridade, disponibilidade e confidencialidade das informações da sua propriedade, além de prevenir, detectar e reduzir a vulnerabilidade a incidentes que tenha relação com o ambiente cibernético, definindo as regras que representam, a nível estratégico, os princípios da Corretora focados no objetivo de segurança da informação.

Princípio da Segurança Cibernética

Acreditamos que os ativos de informação são os bens mais relevantes no mercado financeiro, com isso, é nosso dever tratá-los com responsabilidade. O fundamento da Freex Corretora de Câmbio está no princípio direto a segurança da informação, cujos objetivos constituem a preservação da propriedade da informação, com sua confidencialidade, integridade e

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

disponibilidade, autorizando o uso e compartilhamento de forma controlada, com o monitoramento e tratamento de incidentes oriundos de ataques cibernéticos.

Confidencialidade: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas.

Integridade: garantir que as informações sejam integras, sem modificações indevidas – acidentais ou propositais.

Disponibilidade: garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

Informações Confidenciais

O acesso às informações confidenciais, sendo esses também dados pessoais, coletados e arquivados pela Freex Corretora de Câmbio, deve ser restrito aos profissionais autorizados ao uso direto dessas informações, é necessário a prestação de seus serviços, sendo limitado o uso para outras atividades, deve ser respeitado ainda, o disposto na norma de classificação da informação.

As informações confidenciais devem ser reveladas nas seguintes hipóteses:

- Quando for obrigado a revelá-las através de formalidade legal, ato de autoridade, ordem ou mandado judicial;
- Aos prestadores de serviços autorizados pela Freex Corretora de Câmbio;
- Aos órgãos reguladores do mercado financeiro;
- Para outras instituições financeiras, desde que dentro dos parâmetros legais.

Estrutura de Gerenciamento de Segurança Cibernética

O objetivo do gerenciamento de controles de segurança é assegurar que os procedimentos operacionais sejam elaborados, implantados ou modificados de acordo com os objetivos estabelecidos nesta política.

Gestão de Acesso às Informações

Os acessos as informações são controladas, monitorados, sendo restrito à menor permissão e privilégios possíveis, revisados periodicamente, e cancelados pontualmente ao término do contrato de trabalho do colaborador ou prestador de serviço.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

Os equipamentos e instalações de processamento de informações são mantidos em áreas seguras, com controle incluindo proteção contra ameaças físicas e ambientais.

Os colaboradores são conscientizados através de treinamentos via intranet sobre os conceitos de segurança da informação.

Autenticação

O acesso as informações e aos ambientes tecnológicos da Freex Corretora de Câmbio deve ser permitido apenas às pessoas autorizadas, levando em consideração a segregação de funções.

O controle de acesso aos sistemas deve ser formalizado com os seguintes controles:

- A utilização de login (credencial de acesso) individual, monitorado e passíveis de bloqueios e restrições;
- A exclusão de autorizações dadas a usuários afastados ou desligados da Corretora ou que ainda tenha mudado de função;
- A revisão periódica das autorizações concedidas.

3.3. Política de Gestão de Incidentes

A Política de Gestão de Incidentes tem como objetivo estabelecer princípios, conceitos, diretrizes e responsabilidades sobre os incidentes que possam ocorrer na Freex Corretora de Câmbio e visa orientar o funcionamento do processo de gestão e controle dos incidentes de segurança cibernética e da informação, de forma que estes sejam tratados adequadamente, reduzindo ao máximo os impactos para o negócio. Esta Política tem abrangência corporativa na Corretora, ou seja, afeta todas as suas áreas de negócio, dependências e demais operações no que se refere a ocorrência de incidentes.


Principais Características

A Freex Corretora de Câmbio tem seus processos de Gestão de Incidentes controlados pelas atividades abaixo através de seus responsáveis:

Diretoria

Respalda financeiramente projetos de melhoria da segurança da cibernética.

Área de Riscos ou DPO (Data Protection Officer)

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024


- Analisar casos de violação da segurança, tomando providências imediatas;
- Condução do processo de Gestão de Incidentes de Segurança da Informação;
- Investigação de incidentes, levantamento, cadeia de custódia e segurança das evidências;
- Acompanhamentos dos planos de tratamento junto aos responsáveis pelos incidentes e criação de indicadores e relatórios;
- Comunicação aos gestores responsáveis;
- Realização de análises pós-incidentes para identificação e tratamento de causas raiz e aprimoramento de processos da Corretora e do próprio processo de gestão de incidentes de segurança da informação;
- Prover a divulgação da política de Gestão de Incidentes, bem como das normas e procedimentos vinculados a esta política;
- Estabelecer mecanismos de registro e controle de não conformidade a esta política, reportando-os à Diretoria;
- Obter as informações necessárias para a elaboração do Relatório de Impacto à Proteção de Dados Pessoais;
- Comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular dos dados pessoais a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante a esses dados.

Colaboradores

Devem informar imediatamente, à Área de Riscos todas as violações às políticas de segurança da informação, incidentes, violações de acessos ou anomalias que possam indicar a possibilidade de incidentes, sobre os quais venham a tomar conhecimento.

Infraestrutura e Sistemas

- Provimento dos acessos necessários para que a Área de Riscos possa realizar a identificação e investigação de incidentes de segurança;
- Responsável pelo provimento de trilhas de auditoria e evidencias para a investigação de incidentes;
- Suporte às investigações através do fornecimento de informações e esclarecimentos sobre o ambiente tecnológico e os processos da Área.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

Gestores e DPO - Data Protection Officer


Ao serem notificados sobre incidentes que envolvam recursos ou informações sob sua responsabilidade, devem colaborar com eventuais investigações e tratar os incidentes com a devida urgência e SLA's pré-definidos.

Jurídico

Suporte às questões legais relacionadas a incidentes de segurança da informação.

Processos Gerais

- São considerados Incidentes de Segurança da Informação quaisquer fragilidades ou eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao comprometimento de um ou mais dos princípios básicos de segurança da informação: confidencialidade, integridade, disponibilidade e conformidade, colocando o negócio e seus objetivos em risco.
- Todos os colaboradores devem estar capacitados a identificar incidentes de segurança da informação quando for testemunhado.
- Todos os colaboradores devem notificar qualquer evento de segurança ou fragilidade observada, que possam causar: prejuízos, interrupções, maus funcionamentos, imprecisão ou vazamento de informação nos sistemas da Corretora.
- Vulnerabilidades ou fragilidades suspeitas não deverão ser objeto de teste ou prova pelos colaboradores, sob o risco de violar a política de segurança cibernética e da informação, bem como provocar danos aos serviços ou recursos tecnológicos.
- Todo e qualquer incidente que se caracterize como uma Crise (extrema severidade) deve seguir o Plano de Continuidade de Negócio da Freex Corretora de Câmbio.
- Todos os eventos de incidente de segurança da informação devem ser registrados nos controles e/ou ferramentas para a devida triagem e tratamento.
- Violações ou tentativas de violação da Segurança da Informação, são considerados incidentes de segurança.
- Todos os incidentes de segurança da informação devem ser documentados e comunicados aos gestores responsáveis no momento apropriado.
- O Plano de Comunicação de Incidentes, a gestão de todo o processo de crise, evidências e testes devem estar registrados e armazenados adequadamente, para qualquer tipo de prestação de contas internas e/ou órgão regulador, conforme orientação do documento de Continuidade de Negócio da Freex Corretora de Câmbio.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

O comportamento de possíveis ataques é identificado através de controle de detecção no ambiente com ferramentas de localização de comportamentos maliciosos, Antivírus, AntiSpam, entre outros.

Registro, Análise e Impacto de Incidentes Relevantes

A Área de Tecnologia da Informação é responsável por registrar todos os incidentes ocorridos e destacar para tratamento, aqueles considerados de alto risco para a segurança das atividades da Freex Corretora de Câmbio. A Área de TI identifica quais controles de segurança não foram eficazes, suas causas e impactos a fim de assegurar que novos incidentes não prejudiquem os processos operacionais e de negócio da Corretora.

São analisadas as possibilidades de ações mitigatórias alinhadas aos processos de gestão da continuidade de negócios, apontando os impactos mensurados aos ativos de TI que apoiam os processos de negócio.

Os registros são considerados para efeito de elaboração de cenários para novos testes de incidentes cibernéticos.

Definição dos Parâmetros para Relevância dos Incidentes


Durante a análise de riscos cibernéticos, são adotados parâmetros qualitativos para determinação da relevância dos ativos e dados cibernéticos aos negócios da Freex Corretora de Câmbio.

A tabulação de ativos e sua importância aos processos de negócio da Corretora, suas vulnerabilidades mapeadas e o impacto ao negócio são constantemente revisados por pessoal especializado.

Os sistemas de monitoramento e gestão dos ambientes críticos e incidentes críticos e de grande relevância para a Corretora terão prioridade no seu tratamento. É criada WAR ROOM para o tratamento deste incidente por equipe multidisciplinar incluindo as áreas da Freex Corretora de Câmbio, que estiveram envolvidas no incidente.

Elaboração de Cenário de Incidentes

São definidos cenários de incidentes sobre os ativos considerados prioritários para o negócio, alinhados aos processos operacionais críticos da Freex Corretora de Câmbio. Há o Plano de continuidade dos negócios elaborado com base nas melhores práticas de mercado e que

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

também, considera o uso de cenários de incidentes, sendo periodicamente revisto por meio da metodologia BIA (Análise de Impacto).

Em casos emergenciais os cenários de incidentes e a análise de impactos aos negócios para mitigação de riscos cibernéticos são registrados e apresentados a todos os responsáveis, possibilitando alinhamento sobre o cenário atual de riscos e ações necessárias.

Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes cibernéticos, abrangem, inclusive, informações recebidas de empresas prestadoras de serviços e terceiros.

Plano de Resposta de Incidente de Segurança Cibernética

O procedimento de resposta a incidentes de segurança da informação é composto de etapas necessárias para prover uma abordagem bem definida e organizada para manusear os incidentes de segurança da informação de forma eficiente. Sempre que um evento é reportado como incidente de segurança da informação, o DPO - Data Protection Officer deve acionar o Plano de Resposta a Incidentes de Segurança da Informação para executar atividades apropriadas.

O DPO - Data Protection Officer elaborará relatório anual sobre a implementação e a efetividade do plano de ação e de resposta a incidentes.

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.


Varredura de Vulnerabilidades

As varreduras das redes internas e externas devem ser checadas periodicamente. As vulnerabilidades identificadas devem ser tratadas e priorizadas de acordo com seu nível de reparo.

Redução da Vulnerabilidade

Os processos utilizados para a análise de vulnerabilidades são:

- Atualização do inventário de ativos de TI, com a atribuição de critérios de relevância de cada ativo e de seus dados para os negócios e operações;

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

- Identificação das vulnerabilidades ou ameaças potenciais para cada ativo; e
- Mitigação ou eliminação das vulnerabilidades mais graves dos ativos mais importantes.

Para a análise de vulnerabilidades, a Freex Corretora de Câmbio dispõe de processos e ferramentas especializadas e reconhecidas nos mercados nacional e internacional para:

- Registrar, monitorar e analisar as operações de acesso, a fim de proteger seus registros (logs) e assegurar a devida rastreabilidade;
- Gestão dos acessos às informações por meio de segregação de funções assegurando o controle de acessos de acordo com cada função, para o correto tratamento e processamentos dos dados; e
- Realizar periodicamente testes e varreduras para detecção de vulnerabilidades em sistemas.

Teste de Intrusão e Scan de Vulnerabilidades


- Anualmente são realizados testes de intrusão e scan de vulnerabilidades para a prevenção de vazamento de informações, checagem de proteção contra softwares maliciosos e detecção de aderência de patches de software;
- O escopo é interno e externo, abrangendo sistemas internos de Tecnologia e de Negócios. Farão parte dos testes os firewalls de borda de Internet, testando conexões e IPs externos da rede;
- Apenas empresas especializadas serão contratadas para a execução do trabalho.

Controle Contra Software Malicioso

Computadores e servidores que estejam conectados à rede corporativa ou façam uso das informações da Freex Corretora de Câmbio, devem ser protegidos com uma solução anti-malware determinada pela área de segurança da informação.

Criptografia

Toda resolução de criptografia utilizada na Freex Corretora de Câmbio deve seguir as regras de segurança da informação e os padrões de segurança dos órgãos reguladores.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

Rastreabilidade

Toda informação sensível deve ser identificada, justificado seu uso e receber esta classificação, sendo que as informações classificadas como “sensíveis” devem receber níveis adicionais de proteção e rastreabilidade.

Todos os sistemas que tratam informação classificada como sensível mantém log de acessos de leitura, escrita e alteração são registrados nos concentradores de log com a trilha de auditoria para o tratamento da informação sensível.

São utilizados recursos tecnológicos como criptografia, concentrador de registros (logs) de rede com análise proativa e procedimentos de resposta a incidentes cibernéticos. Estes recursos são continuamente geridos por pessoal específico e especializado.

Processos e procedimentos são adotados pelas áreas de Tecnologia da Informação, Sistemas, e Riscos, a fim de garantir a manutenção da segurança cibernética e manter os riscos cibernéticos sob nível adequado de controle.

Sistemas de autenticação devem ser automatizados para monitorar os seguintes eventos:


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

Desenvolvimento Seguro

A Freex Corretora de Câmbio utiliza de um conjunto de princípios para desenvolver sistemas de forma segura, garantindo que a segurança cibernética seja projetada e implementada no ciclo de vida de desenvolvimento de sistemas.

Backup

A execução de backups é realizada, de forma periódica nos ativos de informação da Freex Corretora de Câmbio de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

Processamento, Armazenamento de dados e Computação em Nuvem

Para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a Freex Corretora de Câmbio assegura-se de um procedimento efetivo aderente às regras previstas na regulamentação em vigor.

A Corretora realizará o tratamento de dados e informações em meio digital por meio de soluções desenvolvidas ou adquiridas pela Corretora, considerando os princípios de segurança da informação: disponibilidade, integridade, confidencialidade, autenticidade, irretratabilidade, privilégio mínimo, necessidade de conhecer, proteção de dados pessoais e proteção da privacidade.

Principais Recomendações de Segurança aos Clientes e Usuários

Autenticação e Senha

- O cliente é responsável pelos atos executados com seu login, que é único e sua senha de uso pessoal e intransferível;
- É importante manter a sua confidencialidade, memorize e não registre a senha em lugar algum. Ou seja, não compartilhar com ninguém e nem anotar em nenhum papel;
- Realizar a alteração de sua senha sempre que existir qualquer suspeita do comprometimento dela;
- Cadastrar senhas de qualidade 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 do ambiente.


Engenharia Social

A engenharia social refere-se à técnica pela qual uma pessoa procura persuadir outra, muitas das vezes abusando da ingenuidade ou confiança do usuário, com o objetivo de ludibriar, aplicar golpes ou obter informações sigilosas.

Phishing

Técnica utilizada por criminosos para enganar os usuários, através de envio de e-mails maliciosos, para obtenção de informações pessoais como senhas, CPF, número de contas etc. As abordagens podem ocorrer das seguintes maneiras:

- Para atrair atenção do usuário, no objetivo de obter alguma vantagem financeira;

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

- Tentam induzir usuários a preencher formulários com os seus dados pessoais ou financeiros, ou até a instalação de softwares maliciosos com o objetivo de coletar informações sensíveis.

Spam

E-mails não solicitados, os quais geralmente são enviados para muitas pessoas, possuindo tipicamente conteúdo com fins publicitários. Além disso, os Spams estão diretamente associados a ataques de segurança, tornando-se um dos principais propagadores de códigos maliciosos, venda ilegal de produtos e disseminação de golpes.

Ligação Falsa

São técnicas utilizadas pelos fraudadores para conseguir informações como dados pessoais, senhas, token, código de identificação do aparelho celular ou qualquer tipo de informação para a prática de fraude.

3.4. Contingência Operacional


Esta política visa estabelecer as diretrizes para a implantação e manutenção de programas de proteção e planos de contingência para os sistemas e ambientes de processamento de dados.

3.4.1. Geral

O Diretor Presidente viabilizará o atendimento da regulamentação vigente, aprovando as diretrizes estabelecidas, que permitam o detalhamento dos programas de proteção e planos de contingência relativos aos sistemas e ambientes de processamento de dados.

As Diretorias deverão:

- Assegurar o cumprimento, no dia a dia, das diretrizes estabelecidas;
- Elaborar e implementar programas e planos de contingência que assegurem a proteção e integridade física dos dados, dos ambientes e equipamentos de processamento e que permitam, em emergências, reação imediata e rápida recuperação das informações, sem prejuízo das rotinas operacionais essenciais à condução dos negócios da Freex Corretora de Câmbio;

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

- Revisar, periodicamente, suas instalações, a fim de assegurar o funcionamento dos sistemas de segurança do local de processamento de dados, tais como sistema de acesso, controles de temperatura e umidade ambiental, extintores etc.;
- Divulgar os programas de proteção e planos de contingência, de forma a assegurar que todos os Funcionários da Corretora, saibam quais são suas funções e responsabilidades em caso de contingência ou desastre;
- Revisar o “Plano de Contingência”, anualmente ou sempre que necessário.

3.5. Política de Privacidade de Dados

A Política de Privacidade de Dados tem como objetivo definir regras e normatizar o serviço de tratamento de dados pessoais dos clientes através de mecanismos tecnológicos específicos disponibilizados pela Freex Corretora de Câmbio, o que se traduz em segurança da informação, em termos de confidencialidade, integridade e disponibilidade, além de total aderência à LGPD. Alicerçada nesse conceito, esta Política se desenvolve aderente a legislação específica para essa atividade e registrada na Lei 13.709/2018, que tem como foco principal a responsabilidade pela guarda e a confidencialidade das informações de cadastro sob responsabilidade da Corretora.


Conceitos e Definições

LGPD: acrônimo para Lei Geral de Proteção de Dados, a qual refere-se a Lei N° 13.709, de 14 de agosto de 2018. Esta lei regulamenta o tratamento de dados pessoais, bem como define os direitos do titular de tais dados.

Dado pessoal: toda e qualquer informação que identifique o titular do dado seja de forma direta (pessoa identificada sem a necessidade de qualquer outra informação extra) ou indireta (pessoa identificável com o auxílio de outras informações).

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, informações de saúde, 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.

Controlador: pessoa natural ou jurídica, de direito público ou privado, responsável pelas decisões de tratamento de dados pessoais, bem como definir os meios e propósitos deste tratamento.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

DPO: acrônimo para Data Protection Officer ou encarregado pela proteção de dados. É o responsável legal pela proteção de dados e programa de privacidade numa empresa perante os órgãos reguladores e governamentais.

ANPD: acrônimo para a Autoridade Nacional de Proteção de Dados Pessoais. É o órgão da administração pública federal responsável por zelar pela proteção de dados pessoais, implementar e fiscalizar o cumprimento da LGPD no Brasil.

Anonimização: processo utilizado para tornar-se um dado passível de não identificação, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Titular(es) dos dados: pessoa física a qual o dado pessoal em tratamento pertence.

Tratamento de dados pessoais: toda atividade realizada com dados pessoais, incluindo, mas não se limitando a atividades como a coleta, compartilhamento, comunicação, acesso, reprodução, processamento, armazenamento, eliminação e alteração de tais dados.

Finalidade: propósito de tratamento de dados que seja legítimo, explícito, delimitado e informado ao titular.


Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.

Informação: Qualquer conjunto de dados que resulte em algum significado compreensível. A informação pode possuir algum valor para a Empresa, seus clientes, parceiros e colaboradores, bem como pode ser de propriedade da Corretora ou estar sob sua custódia.

Colaborador: Entende-se como colaborador qualquer pessoa que trabalhe para a Corretora, quer seja: colaborador com registro em carteira de trabalho, terceiro, estagiário, aprendiz ou trainee.

Gestor: Colaborador que exerce cargo de liderança, como: presidente, vice-presidente, diretores, gerentes, coordenadores, supervisores, líderes ou chefes de seção.

Recurso: Qualquer ativo, tangível ou intangível, pertencente a serviço ou sob responsabilidade da Empresa, que possua valor para ela. Podem ser considerados recursos: pessoas, ambientes físicos, tecnologias, serviços contratados, em nuvem, sistemas e processos.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

A Freex Corretora de Câmbio tem seus processos de Gestão de Privacidade de Dados controlados pelas atividades abaixo, através de seus responsáveis:

- A gestão dos dados, é de responsabilidade de todos os colaboradores, nos limites das atribuições de cada área envolvida;
- Toda manipulação, aquisição ou experimentação de base de dados deverá passar pelo processo de avaliação, previsto pelas Áreas de Controles Internos, Compliance, Riscos e Jurídico, bem como ser formalmente aprovado para tal;
- Em qualquer observação ou constatação de não aderência a essa política, deve ser informada imediatamente às Áreas de Controles Internos, Compliance e Jurídico;
- O processamento deve ser transparente, lícito, justo e deverá manter registros nos sistemas envolvidos;
- Para todos os dados pessoais processados, devem ser feitas as seguintes análises de bases legais: autorização, contrato, obrigação legal, de interesses vitais, público ou interesses legítimos;
- No processamento, deve ser adotada a prática de minimizar os dados, limitados ao que é necessário em relação aos propósitos para os quais são processados;
- No caso de uma violação de segurança, que leve à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais, a Corretora deverá prontamente avaliar o risco para os direitos e liberdades das pessoas e, se apropriado, informar essa violação à autoridade competente.


Atribuições e responsabilidades

Diretoria

- Respalda financeiramente projetos de melhoria da segurança da informação.

Responsabilidades Gerais

- Compete a todos os Colaboradores o cumprimento das diretrizes constantes desta Política;
- Todo colaborador deve aderir formalmente ao Contrato de Segurança.
- Os Colaboradores e demais profissionais com vínculo de trabalho com a Freex Câmbio devem atuar com integridade no exercício de suas funções atentando-se ao Código de Conduta e Política de Segurança da Informação.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

Controles Internos e Compliance

- Promover a divulgação da política de Privacidade de Dados, bem como das normas e procedimentos vinculados a esta política;
- Identificar, com o auxílio da Área de TI, e analisar casos de violação de privacidade e divulgação de informações sensíveis, tomando providências imediatas;
- Realizar trabalhos de análise de vulnerabilidade, com o intuito de aferir e aprimorar cada vez mais o nível de segurança a que se propõe esta política.


DPO - Data Protection Officer ou Encarregado pela Proteção de Dados

- Gestão do Programa de Privacidade;
- Desenvolvimento, manutenção, e propositura de revisão de procedimentos e políticas de privacidade da Freex Câmbio, inclusive desta política;
- Fiscalização do cumprimento de procedimentos e políticas do Programa de Privacidade;
- Programa de treinamento e conscientização em proteção de dados e privacidade;
- Monitoramento do nível de conformidade da Freex Câmbio, por meio de análises de diagnóstico recorrentes, com a definição de planos de ação para melhorar o treinamento e a clareza dos documentos que integram o Programa de Privacidade;
- Atuação como ponto de contato entre o Freex Câmbio e ANPD;
- Atuação como ponto de contato entre a Freex Câmbio e os titulares dos dados;
- Recebimento de requisições e dúvidas dos titulares dos dados;
- Elaboração de Relatórios de Impacto à Proteção de Dados Pessoais, com apuração e revisão dos riscos das atividades.
- Auxiliar os colaboradores da Freex Câmbio e esclarecer-lhes qualquer dúvida sobre o Programa de Privacidade e a forma correta de Tratamento de Dados Pessoais a ser adotada durante a execução de suas atividades.

Princípios de Proteção de Dados

A Lei 13.709/2018 determina que todos os dados utilizados em qualquer processamento devem estar em conformidade com a LGPD, com base no artigo 7º. dessa Lei, que prevê a coleta dos dados pessoais, a qual deve acontecer:

- Mediante o fornecimento de consentimento pelo titular;
- Para o cumprimento de obrigação legal ou regulatória pelo controlador;

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

- Quando necessário para a execução de contrato, ou de procedimentos preliminares relacionados a contrato, do qual seja parte o titular, a pedido do titular dos dados;
- Para a proteção da vida ou da incolumidade física do titular ou de terceiros;
- Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular, que exijam a proteção dos dados pessoais, inclusive quanto ao disposto na legislação pertinente;
- O processamento deve garantir uma adequada segurança dos dados pessoais, incluindo a contramedida de processamento não autorizado ou ilegal, perda acidental, destruição ou danos, se utilizando de técnicas apropriadas.

Utilização dos Dados Coletados

A Freex Câmbio em concordância com a Lei Geral de Proteção de Dados - LGPD, atua com transparência na coleta e processamento de dados pessoais. Deste modo, as finalidades de tratamento estão previstas abaixo:

- Admissão e cadastro no quadro de funcionários e prestadores;
- Processamento das informações junto ao governo federal;
- Obrigações legais junto aos órgãos competentes (Receita Federal e outros);
- Cadastro do Colaborador;
- Cadastro no sistema de acesso físico ao ambiente de trabalho da Freex Câmbio;
- Cadastro nas ferramentas de acesso lógico para desempenho das funções pelas quais o(a) profissional foi contratado(a).


Se necessário, a Freex Câmbio poderá solicitar também dados de funcionários não previstos nesta política para outros fins. Neste caso, a coleta e o tratamento de dados serão suportados por uma base legal prevista na LGPD.

Tratamento de Dados Pessoais

A Freex Câmbio, em conformidade com a LGPD, realizará o tratamento de dados pessoais de acordo com as hipóteses previstas na lei mencionada.

Entre as hipóteses previstas na lei em questão, estão:

- Consentimento fornecido pelo titular;
- Cumprimento de obrigação legal ou regulatória;
- Elaboração de Contrato do qual seja parte o titular, a pedido do titular dos dados;

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

- Exercício regular de direitos em processo judicial, administrativo ou arbitral;
- Atendimento dos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Compartilhamento de Dados

Para viabilizar nossa operação desde a contratação do Colaborador até o fornecimento de salário, benefícios e cumprimentos de obrigações, a Freex Câmbio poderá realizar o compartilhamento de alguns dados pessoais com empresas e órgãos públicos.

Adicionalmente, a Freex Câmbio poderá compartilhar os dados dos Colaboradores com autoridades públicas, tais como autoridades fiscais, fazendárias, judiciárias e policiais, ou terceiros autorizados, se e na medida necessária ou permitida para atender a lei, como:

- Cumprimento de obrigações legais;
- Cumprimento com uma solicitação legal válida e responder a alegações feitas contra a Freex Câmbio;
- Defesa em ações judiciais;
- Resposta a uma solicitação legal válida relacionada à investigações criminais, suspeitas de atividade ilegal ou qualquer outra atividade que possa expor a Freex Câmbio e os titulares de dados a responsabilização legal.

Monitoramento


Alguns dados poderão ser coletados (inclusive por meio de cookies) e serem utilizados para finalidades estatísticas, para o entendimento do perfil de clientes, aprimoramento contínuo dos produtos/serviços e para fins de direcionamento de conteúdo específico.

Os dados irão compor estatísticas sobre o uso do produto/serviço.

Os próprios dados e os resultados estatísticos também poderão ser utilizados para direcionar questões administrativas, comerciais e financeiras da Freex Câmbio, inclusive mediante o direcionamento de campanhas de marketing.

Segurança das Informações

A Freex Câmbio adota medidas técnicas e administrativas em todo o ciclo de vida da informação para a proteção e privacidade dos dados dos titulares, utilizando os melhores esforços para manter a confidencialidade, integridade e disponibilidade.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

Em caso de aquisição, desenvolvimento e manutenção de sistemas, estes devem estar alinhados às melhores práticas de segurança da informação e de privacidade de dados.

Manutenção e Armazenamento dos Dados


Conforme previsto na LGPD, ao fim do processamento de informações os dados devem ser excluídos. Entretanto, há documentos que necessitam sua retenção por período previsto em outras leis ou regulamentações, para isso os dados pessoais dos titulares serão preservados pelo prazo de retenção necessário, considerando para isso as justificativas para tal tratamento:

- Cumprimento de contrato, até o alcance dos objetivos da relação contratual; e
- Cumprimento de obrigação legal, fiscal ou regulatória, pelo prazo indicado em regulamentação aplicável, tais como informações previdenciárias, trabalhistas e outras.
- Se fundamentado no legítimo interesse, que sempre será precedido de uma análise de impacto de privacidade e realizado dentro dos limites da finalidade que o justifica, até que este cesse.

Direitos dos Titulares dos Dados

Os titulares dos dados poderão exercer os seus direitos quanto ao tratamento de seus dados pela Freex Câmbio. Conforme previsto na LGPD, os direitos do titular dos dados são:

- Confirmação da existência de tratamento;
- Acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei;
- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses de retenção para fins legais e regulatórios;
- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

- Revogação do consentimento.

A Freex Câmbio atenderá sempre que possível às solicitações feitas pelos titulares de dados, mas informa previamente que algumas situações podem resultar em atendimento parcial do pedido ou até negativa. Nessas situações, a Freex Câmbio prestará os esclarecimentos e justificativas necessárias.

Relatos de Incidentes

Para o exercício de seus direitos, relato de incidentes ou qualquer comunicação necessária em relação ao tratamento de dados, deve ser contatado o DPO da Empresa.

Para fins de segurança, a Freex Câmbio poderá solicitar algumas informações como parte do procedimento de validação de identidade.

As comunicações serão recebidas pelo DPO, sob gestão do responsável pelo programa de privacidade.

Para fins de conhecimento, em caso de incidentes o processo seguirá conforme previsto na Política de Gestão de Incidentes.


3.6. Política de Gestão de Acessos

A Gestão de Acesso tem como objetivo garantir a preservação e integridade de componentes, processos e informações importantes da Freex Corretora de Câmbio.

Alicerçada nesse conceito esta Política se desenvolve considerando dois pontos básicos relativos à segurança física e, sistemas de informação da Corretora:

Segurança Física – Fornece mecanismos físicos de proteção, que abrangem desde perímetro externo até o espaço interno de trabalho, prevenindo o acesso físico não autorizado, danos, furtos e interferências com as instalações e informações críticas da Corretora.

Sistemas de Informação – Garantir que a segurança é parte integrante de sistemas de informação, identificando os requisitos de segurança na fase de definição de projetos e implementando uma gestão de vulnerabilidade de forma efetiva, sistemática e constante.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

Atribuições e Responsabilidades

Diretoria

- Aprovar a política, bem como suas revisões e adequações;
- Respaldar financeiramente projetos de melhoria da segurança da informação.

Responsabilidades Gerais

Todas as informações trocadas ou armazenadas na Freex Corretora de Câmbio, independentemente de conteúdo, são sua propriedade única e exclusiva. Os usuários devem utilizar os recursos disponibilizados para a condução dos negócios da Corretora.

Gestor de Risco


- Divulgar a importância de sigilo de senhas, bem como o cuidado com seu uso, salientando que ela é sempre de uso pessoal e intransferível, orientando, também, que se deve evitar a utilização de uma mesma senha por um grupo de diversos usuários;
- Analisar casos de violação da segurança, tomando providências imediatas;
- Promover a divulgação da política de Gestão de Acesso, bem como das normas e procedimentos vinculados a esta política;
- Estabelecer procedimentos e realizar a gestão dos sistemas de controle de acesso da Freex Corretora de Câmbio, incluindo processos de concessão, manutenção, revisão e suspensão de acessos aos usuários, conforme Política de Gestão de Acessos;
- Requisitar informações das demais áreas, com o intuito de verificar o cumprimento da política e das Normas.

Conceitos e Definições

Informação: Qualquer conjunto de dados que resulte em algum significado compreensível. A informação pode possuir algum valor para a Corretora, seus clientes, parceiros e colaboradores, bem como pode ser de propriedade da Corretora ou estar sob sua custódia.

Colaborador: Entende-se como colaborador qualquer pessoa que trabalhe para a Corretora, quer seja: colaborador com registro em carteira de trabalho, terceiro, estagiário, aprendiz ou trainee.

Gestor: Colaborador que exerce cargo de liderança, como: presidente, vice-presidente superintendente, diretor, gerente, coordenador, líder ou chefe de seção.


	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

Recurso: Qualquer ativo, tangível ou intangível, pertencente a serviço ou sob responsabilidade da Corretora, que possua valor para a Corretora. Podem ser considerados recursos: pessoas, ambientes físicos, tecnologias, serviços contratados, em nuvem, sistemas e processos.


A Freex Corretora de Câmbio tem seus processos de Gestão de Acesso controlados pelas atividades abaixo através de seus responsáveis:

Segurança Física e Lógica

- Fornece mecanismos físicos de proteção, que abrangem desde perímetro externo até o espaço interno de trabalho, prevenindo o acesso físico não autorizado, danos, furtos e interferências com as instalações e informações críticas da Corretora;
- Definir, controlar e monitorar os perímetros de segurança física das instalações da Corretora, garantindo não haver falhas nem pontos sensíveis para invasões;
- Nenhum indivíduo, não colaborador, deve ter acesso às dependências da Freex Corretora de Câmbio sem que este seja registrado e tenha sua entrada autorizada por um gestor da Corretora;
- É obrigatória a utilização de crachás com controle de acesso às portas, permitindo somente acessos às áreas autorizadas, com os devidos registros;
- É proibido o empréstimo de crachás para terceiros ou mesmo para Colaboradores, pois o crachá é pessoal e intransferível, o não cumprimento desta determinação enseja ao infrator a aplicação de sanção disciplinar;
- As portas devem ter controles de acesso para permitir a entrada somente de pessoas autorizadas;
- Nas instalações da Corretora, todos devem usar a identificação (crachá) de forma visível e devem informar à Gestão de Risco, sobre a presença de qualquer indivíduo não identificado;
- Deve ser criado um mecanismo de acesso de usuários em horários especiais, fora do expediente normal do colaborador, indicando quem teve acesso, data, hora e quem autorizou;
- Equipamentos críticos e componentes críticos da rede devem ser mantidos em salas protegidas e com acessos físico e lógico controlados, devendo ser protegidos contra danos, furtos, roubos e intempéries. O controle de acesso a estas salas deve incluir câmeras, registro de entrada, saída e justificativa;

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024


- Os acessos críticos ao ambiente computacional da Freex Corretora de Câmbio devem ser rastreáveis (logs de eventos);
- Novas solicitações de acesso, fora dos perfis definidos, devem ser aprovadas pelo gestor e avaliadas pela Gestão de Risco, conforme Política de Gestão de Acessos;
- As tentativas de acessos não autorizados devem ser monitoradas e informadas de imediato às Áreas de TI e de Riscos;
- Os usuários devem ter identificação única, pessoal e intransferível, qualificando-os como responsáveis pelas ações realizadas por intermédio desta identificação. Deve-se impedir os acessos simultâneos (“multi-login”);
- A concessão de acessos aos Colaboradores deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação necessários para o pleno desempenho de suas atividades;
- Os processos de trabalho da Corretora devem ser resguardados através da segregação de funções, de forma que atividades não sejam executadas e controladas pelo mesmo colaborador;
- As senhas nunca deverão ser compartilhadas, reveladas a outras pessoas ou escritas, inclusive em programas, e devem ser armazenadas criptografadas nos sistemas;
- Deve-se utilizar o processo de Senha Forte, com senhas formadas por um número mínimo de caracteres alfabéticos e numéricos, com letras maiúsculas e minúsculas, isentas de caracteres idênticos consecutivos;
- Não pode haver repetição de senhas antigas mantidas em histórico definido. O sistema não pode permitir a troca de senhas mais de uma vez por dia e não deve aceitar senhas semelhantes às contidas no histórico;
- Deve-se assegurar que as senhas sejam trocadas periodicamente;
- As senhas iniciais de acesso fornecidas aos usuários devem estar auto expiradas, exigindo a sua troca na primeira utilização;
- As senhas padrões (“default”) de produtos e aplicativos adquiridos devem ser alteradas imediatamente após sua ativação;
- Identificações de usuários devem ser desabilitadas após um número máximo de tentativas inválidas de acesso;
- Deve haver processo de bloqueio automático de identificação de usuário por inatividade. Após um número máximo de dias inativo esta identificação deve ser eliminada do cadastro ativo;

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

- Usuários em férias ou com ausência prolongada, por qualquer outro motivo planejado, devem ter seus acessos bloqueados imediatamente;
- Os direitos de acesso de Colaboradores, terceiros e fornecedores desligados devem ser removidos imediatamente do cadastro;
- Os direitos de acesso de Colaboradores, terceiros e fornecedores que mudaram de função na Corretora devem ser desabilitados na antiga função e validados, novamente, na nova função. Em nenhuma hipótese poderá haver “junção” dos direitos de acesso nesse caso, a não ser que seja uma nova função na Corretora;
- As identificações funcionais (genéricas) devem ter controles de uso que assegurem a segurança da informação e a responsabilidade dos usuários;
- O acesso remoto aos sistemas e aplicativos da Freex Corretora de Câmbio, incluindo o trabalho remoto, deve ser regulamentado e protegido contra o uso não autorizado;
- Deve-se garantir o controle do uso de dispositivos portáteis por meio de política específica;
- Deve-se garantir a identificação automática e o controle de novos equipamentos conectados na rede;
- As permissões de acesso concedidas devem ser revisadas periodicamente pela Área de Riscos e pelo Gestor Imediato do usuário;
- Sessões inativas devem ser automaticamente bloqueadas, por meio de protetores de tela e sua liberação deve exigir senha;
- Deve-se garantir a aderência aos controles de acesso à Internet e Correio Eletrônico (e-mails), definidos em políticas específicas.

Sistemas de Informação – Aquisição, Desenvolvimento e Manutenção

- Os requisitos de segurança devem ser identificados na fase de definição de requisitos de um projeto. Estes requisitos devem refletir o valor para o negócio dos ativos de informação envolvidos e os danos potenciais ao negócio que poderiam resultar em uma falha ou ausência da segurança;
- Os projetos de desenvolvimento de sistemas e aplicações deverão passar pela etapa de arquitetura, interna ou externa. Esta deverá estar alinhada aos objetivos de negócio e aprovada pela Diretoria.
- O acesso aos arquivos de sistemas e aos programas de código fonte deve ser controlado;

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

- Os sistemas devem ser implantados em produção, somente após passarem por testes de homologação pelas áreas responsáveis e após a aprovação do requisitante. Incluem-se, neste caso, sistemas e aplicativos em estações de trabalho;
- Deve-se garantir que planilhas eletrônicas ou qualquer outra aplicação, desenvolvidas em estações de usuários e que farão parte de processo produtivo, sigam o fluxo de controle para implantação em Produção;
- Recursos de “Papel de parede” e “Proteção de tela” devem ser padronizados e homologados;
- Softwares e produtos de mercado devem ter suporte de seus respectivos fabricantes ou representantes devidamente autorizados. Quando descontinuados pelo fabricante não devem ser disponibilizados e as versões já existentes devem passar por processo de análise e substituição;
- Dados e informações “Confidenciais” do ambiente de Produção devem ser mascarados quando disponibilizados em outros ambientes;
- Dados e informações classificadas como “Confidenciais” devem ser criptografadas quando estiverem trafegando fora do ambiente físico da Freex Corretora de Câmbio;
- Deve-se garantir a implantação de processo de aplicação das correções de segurança nos sistemas de informação, visando o gerenciamento de ameaças e vulnerabilidades;
- Garantir a realização de testes periódicos de vulnerabilidade nos sistemas (Teste de Invasão).

3.7. Política de Gestão de Backups


Esta política viabiliza uma atividade fundamental da Continuidade de Negócio e que pressupõe em seu contexto, a Recuperação de Informações na retomada de uma situação de desastre. Considera-se como situação de desastre qualquer situação que afete o processamento de dados da Freex Corretora de Câmbio.

Principais Características

A Freex Corretora de Câmbio tem seus processos de Gestão de Backup controlados pelas atividades abaixo, através de seus responsáveis:

Servidores e máquinas virtuais:

Os backups devem obedecer aos critérios de periodicidade conforme abaixo:

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

- Backups diários (7 versões), sendo que a 8ª substitui a primeira.
- Semanais (6 versões), sendo que a 7ª substitui a primeira.
- Mensais (12 versões), sendo que a 13ª substitui a primeira.
- Semestrais (2 versões), sendo que a 3ª substitui a primeira.
- Anuais (10 versões), sendo que a 11ª substitui a primeira.

Especificamente para Informações relativas aos tributos, os Backups devem ser armazenados por 10 anos por definição da Receita Federal.

Office:

- Backup diário, a cada nova versão salva, é efetuado novo backup em storage, sendo que os dados são armazenados por 1 ano;
- Todos os Backups terão uma cópia adicional enviada para guarda em empresa externa especializada;

Ao desempenharem trabalhos complexos e com finalidades corporativas, todos os Colaboradores deverão gravar o arquivo na rede, como um backup diário;

- É de responsabilidade do usuário o backup dos dados contidos em sua estação de trabalho. Nesse caso, deverá ser realizado backup, no mínimo, semanalmente;
- É importante registrar que todos devem zelar pela confidencialidade, integridade e disponibilidade das informações que tenham acesso, protegendo-as contra utilização e divulgação indevida.

Atribuições e Responsabilidades

Diretoria


Respalda financeiramente projetos de melhoria quando necessários.

Responsabilidades Gerais

Os usuários devem utilizar os recursos disponibilizados pela Freex Corretora de Câmbio para a condução dos negócios da Corretora.

Gestor de Risco

Prover a divulgação da Política de Backup, bem como das normas e procedimentos vinculados a esta política.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

3.8. Política de Cookies

A Política de Gestão de Cookies tem como objetivo disciplinar a utilização de cookies no website e aplicativo da Freex Corretora de Câmbio fazendo a distinção entre os usuários, personalizando as características daquele que navega no website.

Principais Características

Coleta de Informações

Sempre que o website da Freex Corretora de Câmbio é visitado, através dos cookies é possível coletar automaticamente informações sobre:

- Informações técnicas do equipamento, que está sendo utilizado pelo usuário;
- Área de interesse do usuário;
- Preferências pessoais;
- Informações técnicas como o tipo de equipamento que você utiliza, o sistema operacional empregado, o navegador utilizado e o endereço de IP. Estes dados são empregados apenas para fins estatísticos e para aprimorar a experiência de navegação nos portais da Corretora;
- Informações sobre a experiência de navegação em nosso website, como por exemplo as seções visitadas, produtos e serviços visualizados, o tempo de visualização, referências externas, que o levaram ao nosso website etc. Estas informações são empregadas para que se possa aprimorar a estrutura dos portais da Corretora e para eventual direcionamento de ofertas de produtos e serviços;
- Informações sobre suas preferências pessoais, como idioma de navegação e país de origem, utilizado no propósito de adotar essas preferências como padrão a cada nova visita sua em nossos portais.

A Freex Corretora de Câmbio tem seus processos de Cookies definidos para cumprir quatro funções, para as quais estão devidamente autorizados:

Cookies Necessários:

Essenciais para o funcionamento do site. Esse tipo de cookie é definido apenas para resposta a ações feitas pelo usuário, traduzindo-se em solicitação de serviços, como, por exemplo, definir suas preferências de privacidade, efetuar login ou preencher formulários.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

Cookies Funcionais:

Servem para “lembrar” as configurações e preferências feitas pelo usuário, ou ainda ajudar com outras funcionalidades durante a navegação no site.

Cookies de Terceiros:

É possível a disponibilização de conteúdo de terceiros em nossos websites e portais, a exemplo de vídeos, imagens, artigos e pesquisas de serviços de mídia social como Instagram, LinkedIn, Facebook etc.

Ao acessar o conteúdo desses provedores, é provável que cookies destes terceiros sejam igualmente instalados em seus dispositivos.

A Corretora não possui gerência ou controle sobre o uso, finalidade e funcionamento destes cookies.

Recomendamos que busque conhecer a política de cookies desses provedores para mais informações.

A Freex Corretora de Câmbio disponibiliza a funcionalidade de compartilhamento de página ou conteúdo em seus websites que permitem a divulgação de conteúdo compartilhado em plataformas como Facebook, Instagram, LinkedIn, WhatsApp, Twitter e outros. Estes serviços de terceiros poderão, igualmente, instalar cookies, quando você acessa estes serviços.

Atribuições e Responsabilidades


Diretoria

Respalda financeiramente projetos de melhoria da segurança da informação.

Responsabilidades Gerais

- Os usuários devem utilizar os recursos disponibilizados pela Freex Corretora de Câmbio para a condução dos negócios da Corretora;
- Compete a todos os Colaboradores o cumprimento das diretrizes constantes desta Política.

Governança de T.I.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

- Responsável pela criação das políticas, normas e procedimentos da Política de Gestão de Cookies;
- Prover a divulgação da política de Gestão de Cookies, bem como das normas e procedimentos vinculados a esta política.

3.9. Política de Gestão de Ativos

A Política de Gestão de Ativos tem como objetivo estabelecer padrões para que os ativos de tecnologia da informação da Freex Corretora de Câmbio sejam identificados.

Principais Características

A Corretora tem seus processos de Gestão de Ativos controlados pelas atividades abaixo através de seus responsáveis:

Grupo de Ativos

Esta Política leva em consideração os ativos separados pelos seguintes grupos:

Ativos intangíveis: A marca e a reputação da Corretora, por exemplo, aquilo que não é constituído de um bem material físico.

Ativos físicos: Equipamentos, que compõem os recursos de tecnologia e de informática, como computadores, mídias removíveis, equipamentos de comunicação e conectividade, entre outros e suas respectivas instalações.

Ativos de softwares: Os programas, sistemas, ferramentas e utilitários adquiridos ou desenvolvidos pela Corretora e que fazem parte das atividades, em seu dia a dia.

Ativos de serviço: Equipamentos de infraestrutura como eletricidade, ventilação, controle de umidade, entre outros.

Ativos de informação: São dados em tráfego ou armazenados em sistemas de informação, estejam estes em formato lógico (elétrico, magnético ou ótico) ou físico (impressos). Política de Segurança da Informação da Freex Corretora de Câmbio.

Consideramos ativos de tecnologia da informação, da Corretora, os ativos físicos, ativos de softwares e os ativos de informação. Nesta política serão considerados os ativos físicos e de software.

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

Ciclo de Vida

Um processo de gestão de ativos deve ser estabelecido e documentado, para garantir que os ativos de tecnologia da informação sejam gerenciados e monitorados;

O processo de gestão de ativos deve levar em consideração as fases do ciclo de vida do ativo:

Planejamento: Fase de alinhamento das ações com a estratégia corporativa. Esta fase envolve a revisão dos ativos, que são atualmente usados em toda a organização e análise dos custos de compra e instalação de novos ativos de TI.

Aquisição: Fase de definição do padrão técnico, empresas fornecedoras, contratações e estabelecimento de acordo contratuais.

Implantação: Fase de configuração/instalação técnica e disponibilização conforme padrões estabelecidos.

Gerenciamento: Fase de controle, apoio técnico, manutenção, atualização e monitoração.

Descarte: Processo realizado quando um bem perde sua utilidade e torna-se antieconômico. Esta fase corresponde à transferência de um bem para outra categoria, que são: material obsoleto, inservível ou excedente.

Inventário: Os ativos de tecnologia da informação da Freex Corretora de Câmbio devem ser inventariados, claramente identificados e registrados.

A Área de Infraestrutura da Freex Corretora de Câmbio tem a responsabilidade de realizar periodicamente os inventários e armazenar os resultados por um período de 2(dois) anos para fins de auditoria interna. Periodicamente deve haver uma revisão pela área técnica de segurança da informação para assegurar que os ativos de tecnologia da informação da Corretora estejam em conformidade com o inventário.

Uso Aceitável

- Os ativos de tecnologia da informação da Freex Corretora de Câmbio são destinados para uso das atividades relacionadas ao trabalho da Corretora, assim, devem ser utilizados para este fim por seus respectivos usuários e responsáveis;
- Os usuários devem estar atentos aos princípios de segurança da informação (Confidencialidade, Integridade e Disponibilidade) e perfeito funcionamento na utilização dos ativos de tecnologia da informação;

	POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO	Edição	1
		Versão	1
		Ano	2024
		Publicação	02/09/2024

- Os usuários devem manter a integridade (configurações) dos ativos físicos e de software da Corretora. Caso seja necessário, deverá entrar em contato com a Central de Serviços, que acionará as áreas responsáveis com prerrogativa para realizar estas atividades;
- Os ativos de tecnologia da informação da Freex Corretora de Câmbio disponibilizados devem ser cadastrados e configurados, com identificação única, padrões mínimos de segurança e usuário responsável pelo uso, no intuito de serem homologados e incorporados na rede corporativa.

Boas Práticas

- Sempre que possível, os ativos físicos portáteis (notebooks, celulares etc.) devem permanecer nas instalações da Freex Corretora de Câmbio para evitar exposição e risco de furto ou roubo;
- É recomendável que ao trafegar com ativos físicos portáteis (notebooks, celulares etc.) da Corretora, estes sejam devidamente protegidos, guardados em locais seguros ou não expostos;
- Em aeroportos ou taxis, recomenda-se que ativos físicos portáteis (notebooks, celulares etc.), sempre estejam sob sua visão e guarda.