guru / CTVM

Política de Segurança Cibernética

VERSÃO 01 · APROVADO EM 17.12.2025 · DOCUMENTO PÚBLICO

POLÍTICA DE SEGURANÇA CIBERNÉTICA

IDENTIFICAÇÃO DO DOCUMENTO

Versão	Data de Publicação	Vigente até	Área Responsável	Código
01	17/12/2025	17/12/2026	Tecnologia	POL-001

PÚBLICO-ALVO

As diretrizes dispostas nesta política de segurança cibernética ("**Política**") deverão ser observadas por todos os administradores, diretores, funcionários, estagiários, prestadores de serviços e partes relacionadas da Guru Corretora de Títulos e Valores Mobiliários Ltda. ("**Guru CTVM**"), da Guru Desenvolvimento de Software Ltda., da Guru Serviços Digitais Ltda. e da Guru Participações Ltda. (todas em conjunto, "**Guru**" ou "**Grupo Guru**"), bem como qualquer pessoa (física ou jurídica) que tenha acesso a informações, equipamentos, sistemas, processos e ambientes da Guru, designadas nesta Política, em conjunto, como "**Colaboradores**".

RESUMO

A presente **Política**, desenvolvida de acordo com diretrizes do Banco Central e da CVM, principalmente em conformidade com o disposto na Resolução BCB nº 85/21 e na Resolução BCB nº 538/25, na Resolução CVM nº 35/21 e na Lei nº 13.709, de 14 de agosto de 2018, é **norteada pelos princípios** da **confidencialidade**, que garantirá que todas as informações tratadas sejam de conhecimento exclusivo de pessoas autorizadas; da **integridade**, que garantirá que as informações permaneçam íntegras; e da **disponibilidade dos dados e dos sistemas**, que permitirá que as informações sejam disponibilizadas para aqueles que possuam autorização para tratá-las.

Além disso, esta Política tem como intuito assegurar a aplicação dos princípios de **proteção e segurança cibernética** de clientes, parceiros, terceiros, profissionais ou qualquer instituição

ou pessoa que tenha relacionamento com o Grupo Guru, bem como possibilitar a **prevenção, detecção e redução da vulnerabilidade a incidentes** relacionados com o ambiente cibernético.

1. DEFINIÇÕES

Os seguintes termos, quando utilizados ao longo desta Política, possuirão os significados abaixo:

Banco Central: Banco Central do Brasil.

Cliente: todos os usuários dos produtos e serviços da Guru CTVM.

CMN: Conselho Monetário Nacional.

Colaborador: todos os administradores, diretores, funcionários, estagiários, eventuais prepostos, prestadores de serviços e partes relacionadas do Grupo Guru, bem como qualquer pessoa (física ou jurídica) que tenha acesso a informações, equipamentos, sistemas, processos e ambientes da Guru.

Controle: qualquer recurso ou medida que assegure formas de tratamento, redução, eliminação ou transferência de Riscos. A implantação e a manutenção adequada de Controles materializam a Segurança da Informação. Podem ser interpretados como Controles: políticas, processos, rotinas, procedimentos, estruturas organizacionais, técnicas padrão, *software*, *hardware* e outros.

CVM: Comissão de Valores Mobiliários.

Dados Pessoais: informações relacionadas à pessoa natural identificada ou identificável.

Encarregado: significa a pessoa indicada para atuar como canal de comunicação entre a Guru CTVM e os titulares de Dados Pessoais e a Autoridade Nacional de Proteção de Dados - ANPD.

Gestor: qualquer Colaborador que exerce cargo de liderança, incluindo, mas não se limitando a, diretor, superintendente, *head* de área, gerente, coordenador, líder etc.

Grupo Guru ou Guru: Guru Corretora de Títulos e Valores Mobiliários Ltda., Guru Desenvolvimento de Software Ltda., Guru Serviços Digitais Ltda. e Guru Participações Ltda.

Informação: qualquer conjunto organizado de dados que possua algum propósito e valor para a Guru, seus clientes, Prestadores de Serviços e/ou Colaboradores. A Informação pode ser aquela de propriedade da Guru que esteja sob sua custódia ou sob custódia de terceiros. A Informação pode envolver também dados relacionados a pessoas físicas identificadas ou identificáveis, os Dados Pessoais.

Incidentes de Segurança: quaisquer 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. Violações ou tentativas de violação desta Política ou de Controles de Segurança da Informação, intencionais ou não, são considerados Incidentes de Segurança.

Incidentes de Segurança Envolvendo Dados Pessoais: quaisquer Incidentes de Segurança envolvendo Dados Pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento inadequado ou ilícito de Dados Pessoais.

Lei nº 13.709/18: Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados - LGPD.

Prestadores de Serviços: significam as empresas contratadas para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem à Guru CTVM.

Relatório Anual: o relatório anual sobre a implementação do Plano de Ação e Resposta a Incidentes de Segurança.

Resolução BCB nº 85/21: Resolução BCB nº 85, de 8 de abril de 2021, conforme alterada.

Resolução BCB nº 538/25: Resolução BCB nº 538, de 18 de dezembro de 2025, que altera a Resolução BCB nº 85/21, estabelecendo controles adicionais de segurança cibernética para

instituições de pagamento, corretoras e distribuidoras de títulos e valores mobiliários.

Resolução CVM nº 35/21: Resolução CVM nº 35, de 26 de maio de 2021, conforme alterada.

Riscos: quaisquer eventos que se materializados possam afetar a capacidade da Guru CTVM de atingir seus objetivos e suas estratégias de negócio e/ou causar danos financeiros e/ou reputacionais à Guru e/ou prejudicar a continuidade de suas atividades.

Riscos Cibernéticos: os Riscos oriundos de *malware*, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, entre outros, que possam expor banco de dados, redes e sistemas da Guru.

Segurança Cibernética: o conjunto de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, orientações, abordagens de gestão de Riscos, ações, treinamentos, melhores práticas, seguros e tecnologias que podem ser usados para proteger o ambiente cibernético, a organização e as propriedades de usuários(as).

Segurança da Informação (SI): a proteção das Informações, sendo caracterizada pela preservação de:

a. Confidencialidade: garantia de que a Informação somente será acessada por pessoas efetivamente autorizadas;

b. Integridade: garantia de que a Informação somente será modificada por pessoas efetivamente autorizadas a fazê-lo e de acordo com os métodos aprovados para estas ações;

c. Disponibilidade: garantia de que os Colaboradores autorizados obtenham acesso à Informação e aos sistemas correspondentes sempre que necessário, nos períodos e em ambiente aprovados pela Guru; e

d. Conformidade: garantia de que Controles de Segurança da Informação, devidamente estabelecidos, estão sendo executados conforme esperado e produzindo resultados efetivos no cumprimento de seus objetivos.

TI: significa tecnologia da informação.

2. OBJETIVO

Esta Política tem como objetivo demonstrar a capacidade da Guru CTVM em:

(i) Cumprir com a legislação e a regulamentação de Segurança Cibernética em vigor;

(ii) Preservar a confidencialidade, a integridade, a conformidade e a disponibilidade dos dados e dos sistemas de informações utilizados em sua operação;

(iii) Prevenir, detectar e reduzir vulnerabilidades relacionadas a Incidentes de Segurança, conforme melhores práticas de Segurança Cibernética, incluindo procedimentos de Controles que abrangem a autenticação, a criptografia, a prevenção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, conforme aplicável, o estabelecimento de mecanismos de rastreabilidade, os Controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações;

(iv) Estabelecer medidas técnicas e administrativas, no tocante a processamento e armazenamento, capazes de proteger as informações, inclusive Dados Pessoais, contra acessos não autorizados e de situações acidentais ou ilícitas envolvendo a destruição, a perda, a alteração, a comunicação ou o vazamento de Informação; e

(v) Definir Controles para a gestão dos Riscos de Segurança da Informação.

Para elaboração desta Política, levou-se em conta o porte, o perfil de risco e o modelo de negócios da Guru CTVM, assim como a natureza de suas operações, a complexidade dos seus produtos, serviços, atividades e processos, além da classificação dos dados e informações sob sua responsabilidade e utilizados no curso de suas atividades.

3. PRINCÍPIOS

A Guru CTVM está comprometida em manter padrões adequados de Segurança Cibernética em linha com as melhores práticas de mercado e, por isso, adota os princípios abaixo:

(i) Confidencialidade: garantia de que todas as Informações apenas são acessadas por pessoas autorizadas, sendo o acesso a elas limitado;

(ii) Integridade e autenticidade: garantia de que todas as Informações são precisas, completas, verdadeiras e protegidas de alterações e/ou mutações indevidas, intencionais ou acidentais, sendo mantidas em seu estado original;

(iii) Disponibilidade: garantia de que pessoas autorizadas tenham acesso à Informação de forma precisa, completa, verdadeira e protegida de alterações indevidas, intencionais ou acidentais;

(iv) Proteção da Informação: todo produto ou informação gerada, processada, transmitida, armazenada por qualquer Colaborador constitui ativo e propriedade intelectual da Guru CTVM, essencial à condução de seus negócios. Independentemente da forma apresentada que pode ser de forma física, eletrônica, escrita ou falada ou como ela é compartilhada, armazenada ou transmitida, a informação deve ser utilizada unicamente à finalidade à qual foi autorizada pelo Gestor da informação e não deve ser utilizada em meios não autorizados. É diretriz que toda informação de propriedade da Guru CTVM seja protegida de forma a não comprometer a sua confidencialidade, integridade ou disponibilidade;

(v) Gestão e controle de acessos: o acesso e o uso de todos os sistemas de informação, diretórios de rede, bancos de dados, mensagens instantâneas, acesso à Internet e demais recursos devem ser restritos a pessoas autorizadas pelo Gestor (e quando aplicável pelo proprietário da informação) responsável conforme a necessidade mínima ao cumprimento de suas funções, além disso, são monitorados e rastreados através de logs fornecidos pelos sistemas de informação e mecanismos de prevenção a vazamentos de dados. O acesso às informações e aos ambientes tecnológicos da Guru CTVM deve ser permitido apenas às pessoas autorizadas pelo proprietário da informação, levando sempre em consideração o princípio do menor privilégio, a segregação de funções conflitantes e a classificação da informação. O controle de acesso aos sistemas sempre deverá ser formalizado junto à Guru

CTVM e contemplar, no mínimo, os seguintes controles: (i) identificadores individualizados (credencial de acesso), tais controles devem ser monitorados e, ainda, passíveis de bloqueios e restrições (automatizados e manuais); (ii) remoção de autorizações dadas a usuários cuja função tenha mudado ou tenham sido afastados ou desligados da Guru CTVM; e (iii) revisão periódica das autorizações concedidas;

(vi) Acesso a sistemas: todo e quaisquer acessos às informações são controlados, monitorados e restringidos à menor permissão e privilégios possíveis, revistos periodicamente. Além disso, os acessos são cancelados tempestivamente ao término do contrato de trabalho do Colaborador ou do Prestador de Serviços. Os equipamentos e instalações de processamento de dados e informação crítica e/ou sensível são mantidos em áreas seguras, com controle de acesso apropriado e proteção contra ameaças físicas e ambientais. O uso esporádico e responsável para fins pessoais é permitido, à medida que não interfira no trabalho do Colaborador ou implique conflito de interesses da Guru CTVM;

(vii) Rastreabilidade: devem ser implantadas trilhas de auditoria automatizadas para todos os componentes de sistema, com a finalidade de reconstruir os seguintes eventos: (i) autenticação de usuários (tentativas válidas e inválidas); (ii) acesso a informações; e (iii) ações executadas pelos usuários, incluindo criação ou remoção de objetos do sistema;

(viii) Recursos de rede: computadores conectados à rede corporativa não devem ser acessíveis diretamente pela Internet. Além disso, não é permitida a conexão direta de rede de terceiros utilizando-se protocolos de controle remoto aos servidores conectados diretamente na rede corporativa. Para solicitação de criação, alteração e exclusão de regras nos firewalls e ativos de rede, o requisitante deve encaminhar pedido à área de Segurança Cibernética, que fará a análise e aprovação, enviando para que seja executada pela área de Tecnologia da Informação;

(ix) Credenciais de acesso: todo Colaborador é responsável por todos os atos executados com seu identificador (login/sigla de acesso e senha) que é único, pessoal e intransferível para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia. Além disso, o Colaborador deve impedir o uso de seu equipamento por outras pessoas enquanto este estiver logado e não usar as credenciais de acesso de outros Colaboradores e bloquear a estação de trabalho ao se ausentar. O acesso às informações confidenciais, incluindo Dados Pessoais, coletadas e armazenadas pela Guru CTVM é restrito

aos profissionais autorizados, sendo limitado o uso para outras tarefas. Além disso, as definições de classificação da informação previstas devem ser respeitadas. A Guru CTVM preza pela privacidade das informações no âmbito da Lei Geral de Proteção de Dados - LGPD e da Política de Privacidade da Guru;

(x) Prevenção contra vírus, arquivos e softwares maliciosos: a Guru CTVM possui Controles para prevenir que vírus e outros tipos de arquivos maliciosos entrem e espalhem-se nos sistemas e servidores através de softwares não homologados, cuja instalação e uso são proibidos por colocarem em Risco a Segurança das Informações. Todos os ativos (computadores, servidores, entre outros dispositivos) que estejam conectados à rede corporativa ou façam uso de informações da Guru CTVM devem, sempre que compatível, ser protegidos com uma solução antimalware determinada pela área de Segurança da Informação;

(xi) Manutenção e cópias de segurança: o processo de execução de backups é realizado, periodicamente, nos ativos de informação da Guru CTVM, de forma a evitar ou minimizar a perda de dados diante da ocorrência de Incidentes de Segurança. A Guru CTVM possui política e procedimentos específicos para garantir a recuperação de dados e informações;

(xii) Classificação de dados e informações: a Guru CTVM possui procedimentos específicos para garantir as categorias para efeitos de classificação da informação;

(xiii) Desenvolvimento seguro e criptografia: a Guru CTVM mantém 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. Ainda, possui procedimentos específicos relativos à prática de desenvolvimento seguro de sistemas e criptografia. Toda solução de criptografia utilizada na Guru CTVM deve seguir as regras de Segurança da Informação e, também, os padrões de segurança estabelecidos pelos órgãos reguladores;

(xiv) Melhoria contínua: garantia de que serão implementados os melhores esforços para uma melhoria contínua dos Controles relacionados à Segurança Cibernética;

(xv) Promoção de um ambiente positivo de segurança: promoção do engajamento contínuo e constante de todos os Colaboradores e Prestadores de Serviços em desempenhar

suas atividades de acordo com os parâmetros de segurança estipulados nesta Política, por meio de medidas educativas e de conscientização;

(xvi) Uso de justificativa legal: garantia de que os Dados Pessoais são tratados pela Guru apenas quando houver uma justificativa legal;

(xvii) Transparência: garantia de transparência aos titulares de Dados Pessoais a respeito de quais e como os seus respectivos Dados Pessoais são tratados pela Guru; e

(xviii) Minimização: garantia de tratamento apenas de Dados Pessoais estritamente necessários para o atingimento de finalidades específicas.

4. DIRETRIZES

Para efetivar os princípios apresentados anteriormente nesta Política, garantido as melhores práticas de mercado relacionadas à Segurança Cibernética, foram determinadas diretrizes que buscam proteger a Guru CTVM contra o eventual vazamento de Informações, bem como contra fraudes e indisponibilidade de sistemas. Tais diretrizes devem ser seguidas por todos os Colaboradores e Prestadores de Serviços. São elas:

4.1. Aquisição de Tecnologia da Informação (TI)

Todas as contratações, os desenvolvimentos de sistemas e as manutenções periódicas de TI são centralizadas e gerenciadas pelos membros do Comitê de Riscos da Guru CTVM, do qual fará parte o Diretor de Tecnologia e Segurança Cibernética e o Encarregado da Guru CTVM.

Os recursos de TI adquiridos pela Guru CTVM devem ser inventariados, controlados e disponibilizados de acordo com as boas práticas de Segurança da Informação.

4.2. Contratação de Prestadores de Serviços

Antes da contratação de um Prestador de Serviços, em especial daqueles de processamento e armazenamento de dados e de computação em nuvem, deverá ser realizado um processo de due diligence pelo Comitê de Riscos, que aprovará ou não a contratação.

Todos os contratos de prestação de serviços firmados pela Guru CTVM com terceiros devem conter cláusulas de confidencialidade e responsabilidade pela proteção da Informação e não divulgação, de forma que o respectivo sigilo perdure mesmo após o encerramento da prestação de serviços.

Na contratação de Prestadores de Serviços de processamento e armazenamento de dados e de computação em nuvem, no Brasil ou no exterior, o responsável deve comunicar ao Banco Central em até 10 (dez) dias após a contratação do respectivo serviço, as seguintes informações: (i) denominação da empresa; (ii) serviços que serão prestados; e (iii) países e regiões onde os serviços serão prestados e os dados poderão ser armazenados, processados e gerenciados.

A contratação de um Prestador de Serviços pela Guru CTVM está condicionada à observância dos seguintes requisitos mínimos:

(i) Existência de governança corporativa no Prestador de Serviços de acordo com a relevância do serviço prestado e os Riscos existentes, considerando a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados;

(ii) Cumprimento pelo Prestador de Serviços da legislação e regulamentação em vigor;

(iii) Disponibilização à Guru CTVM dos dados processados e armazenados pelo Prestador de Serviços;

(iv) Disponibilização à Guru CTVM dos relatórios elaborados por auditoria externa;

(v) Implementação de Controles pelo Prestador de Serviços voltados à confidencialidade, à integridade, à disponibilidade e à recuperação de dados e informações processadas ou armazenadas;

(vi) Aderência a certificações exigidas de acordo com o mercado em que o Prestador de Serviços atua;

(vii) Disponibilização de informações pelo Prestador de Serviços para o monitoramento pela Guru CTVM dos serviços prestados;

(viii) Segregação pelo Prestador de Serviços de dados e informações de clientes e usuários da Guru por meio de Controles físicos e lógicos;

(ix) Implementação pelo Prestador de Serviços de Controles de acesso voltados à proteção dos dados dos usuários finais; e

(x) Existência de convênio firmado entre Banco Central com as autoridades supervisoras dos demais países nos quais os serviços são prestados.

No caso de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, a Guru deverá observar os seguintes requisitos:

(i) Assegurar a existência de convênio para troca de informações entre o Banco Central e as autoridades supervisoras dos países onde os serviços poderão ser prestados;

(ii) Assegurar que a prestação dos serviços não cause prejuízos ao seu regular funcionamento, nem embaraço à atuação do Banco Central;

(iii) Definir, previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;

(iv) Prever alternativas para a continuidade dos serviços prestados, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços; e

(v) Observar os dispositivos referentes à transferência internacional de Dados Pessoais nas leis e regulamentações aplicáveis ao assunto, incluindo, mas não se limitando à Lei nº 13.709/18.

No caso da execução de aplicativos por meio da Internet, a Guru assegurará que o potencial Prestador dos Serviços adote Controles que mitigam os efeitos de eventuais vulnerabilidades

na liberação de novas versões do aplicativo.

A contratação, bem como alterações contratuais significativas, de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deverão ser comunicadas ao Banco Central.

4.3. Comportamento Seguro

Todas as Informações de propriedade ou sob custódia da Guru CTVM devem ser utilizadas tão apenas para o estrito cumprimento dos seus interesses, na forma da legislação e regulamentação vigente. Desse modo, todos os Colaboradores devem assumir um comportamento seguro para evitar eventuais exposições das Informações a terceiros não autorizados, independentemente do local em que a Informação esteja armazenada ou do meio pelo qual ela for transmitida.

Ademais, é vedado aos Colaboradores emitir, sem prévia autorização, opiniões em nome da Guru CTVM e todos são responsáveis por manter as Informações da Guru CTVM em locais seguros, não deixando documentos nas impressoras e bloqueando seus dispositivos quando se ausentar de suas estações de trabalho.

Por fim, o descarte de Informações sigilosas contidas em qualquer meio, seja impresso ou eletrônico, deve ser feito de forma segura, garantindo a destruição dos dados de forma que não possam ser novamente recuperados.

4.4. Conscientização e Divulgação da Política

Para a devida conscientização, esta Política será amplamente divulgada por meio de programas de capacitação obrigatórios ministrados para todos os Colaboradores (o que inclui eventuais prepostos, bem como prestadores de serviço) anualmente ou em menor periodicidade, conforme necessário. A divulgação desta Política será realizada de maneira clara e objetiva a todos Colaboradores (o que inclui eventuais prepostos, bem como prestadores de serviço) do Grupo Guru e ela ficará disponível na Intranet da instituição, bem como no site da instituição.

A realização de curso de atualização e revisão acerca dos temas de Segurança Cibernética,

com avaliação de aproveitamento, é obrigatória a todos os Colaboradores (o que inclui eventuais prepostos, bem como prestadores de serviço), devendo ser feita anualmente, ou sempre que ocorrerem atualizações nos sistemas que exijam treinamento específico do usuário. Os cursos serão sucedidos por avaliações também periódicas.

O treinamento contemplará, sobretudo, o tema de Segurança da Informação, com um programa efetivo de conscientização e disseminação da cultura de Segurança Cibernética. Dependendo da atividade executada na Guru CTVM, treinamentos adicionais podem ser necessários em questões de Segurança Cibernética.

Como parte do treinamento mencionado acima, serão realizados com todos os Colaboradores exercícios de phishing ético. Esses exercícios são projetados para replicar táticas que os cibercriminosos usam para tentar acessar as redes, sistemas e informações da Guru CTVM. O objetivo do exercício de phishing ético educacional é promover a conscientização de atividades criminosas, bem como treinar e educar Colaboradores na identificação de phishing e relato de mensagens suspeitas.

Os resultados desses exercícios (taxas de cliques e relatórios) são projetados para ajudar o Colaborador a entender seu nível de resiliência cibernética e Risco. O feedback sobre esses exercícios será fornecido aos Colaboradores por e-mail. A realização dos testes de phishing ético torna possível medir a boa gestão de Riscos por parte dos Colaboradores, o que também pode determinar a necessidade de ações adicionais que permitam melhorar a gestão de Riscos.

A tabela abaixo traz um resumo dos nossos programas de capacitação obrigatórios, sua abrangência, sua frequência, métodos de medição da aderência e, caso aplicável, planos de ação a serem adotados:

Tipo	Abrangência	Frequência	Métodos de Medição da Aderência	Planos de Ação
Treinamento de Conscientização Geral	Colaboradores em geral (o que inclui eventuais prepostos, bem como prestadores de serviço)	Anual	Questionários, análise de desempenho	Reforçar os temas nos próximos treinamentos, se necessário
Simulações de Phishing	Colaboradores em geral (o que inclui eventuais prepostos, bem como prestadores de serviço)	Semestral	Taxa de cliques e relatórios	Ações corretivas, como treinamentos adicionais personalizados
Simulação Prática de Resposta a Incidentes de Segurança, conforme item 7 desta Política	Colaboradores encarregados do tema determinados anualmente pelo Diretor de Tecnologia e Segurança Cibernética	Anual	Avaliação de desempenho em simulações e relatórios de resposta	Ajustar procedimentos com base nas lições aprendidas
Workshop sobre Boas Práticas de Segurança	Colaboradores em geral (o que inclui eventuais prepostos, bem como prestadores de serviço)	Anual	Pesquisa de feedback e casos práticos	Revisão e atualização dos conteúdos abordados

4.5. Gestão de Acesso aos Sistemas

O acesso a todo e qualquer sistema tecnológico da Guru CTVM por usuários internos (e.g., Colaboradores) e externos (e.g., Clientes) deve ser autenticado, ou seja, protegido por credenciais de identificação. As credenciais de identificação são compostas por usuário e senha. Ademais, são de uso exclusivo pessoal e intransferíveis, sendo o titular das credenciais de identificação integral e pessoalmente responsável pelas ações realizadas com referidas credenciais, seja perante a Guru seja perante terceiros.

A Guru CTVM adota a seguinte **política no tocante a senhas**, considerando as características do seu negócio e as melhores práticas de mercado:

- criação de “senha forte”, com os seguintes requisitos obrigatórios:
  - Letras maiúsculas e minúsculas
  - Números
  - Caractere especial (%@#$&)
  - No mínimo 12 dígitos
  - Não deve ser igual a alguma senha já utilizada
- atualização periódica de senhas;
- para acesso aos sistemas transacionais online, adoção de duplo fator de autenticação.

Mais informações estão disponíveis no documento Boas Práticas Segurança da Informação.

No que diz respeito aos Colaboradores, as credenciais de identificação são concedidas para uso individual e restrito em atividades relacionadas aos serviços prestados enquanto perdurar a prestação de serviços para a Guru CTVM. Ademais, são de uso exclusivo pessoal e intransferíveis, portanto, o seu compartilhamento é estritamente proibido.

Todos os perfis de usuários e acessos a Informações devem ser revisados periodicamente, seguindo os seguintes parâmetros (i) gestão de acessos, (ii) classificação das Informações e (iii) segregação de funções, observando os princípios de mínimo acesso (*least privilege*) e de necessidade de conhecimento (*need to know*). As senhas dos Colaboradores serão atualizadas trimestralmente.

A partir das credenciais de identificação, todas as ações, ainda que remotas, de

Colaboradores são monitoradas, de forma a possibilitar a identificação e a responsabilização do titular das credenciais pelas ações realizadas.

Para manutenção de sigilo e confidencialidade, o desligamento de um Colaborador acarreta, automaticamente, o encerramento de todos os seus acessos aos sistemas tecnológicos da Guru.

4.6. Varredura de Vulnerabilidades e Testes de Invasão

A Guru CTVM deve ter equipe interna especializada e/ou contratar periodicamente consultoria com certificação técnica para realização de atividades referentes a varreduras de vulnerabilidades em todo o seu ambiente interno e, também, para realização de testes de invasão *(pen tests)*, devendo ser adotados os seguintes procedimentos:

(i) Desenvolvimento e implementação de metodologia para testes de invasão, incluindo testes de invasão externa e interna pelo menos anualmente e após qualquer atualização ou modificação significativa;

(ii) Monitoramento de todo o tráfego no perímetro do ambiente de dados, bem como em pontos críticos dentro do ambiente de dados, com envio de alertas na ocasião de eventos suspeitos; e

(iii) Implementação de processo para responder a quaisquer alertas gerados pela solução de detecção de alterações.

Ao fim desses testes, será apresentado um relatório independente, a partir do qual o Comitê de Riscos deverá definir plano de ação corretivo às eventuais vulnerabilidades identificadas, que deverão sempre ser tratadas e priorizadas de acordo com a classificação de criticidade para sua resolução.

4.7. Controles Adicionais — Resolução BCB nº 538/2025

Em observância à Resolução BCB nº 538, de 18 de dezembro de 2025, que alterou a Resolução BCB nº 85/21, a Guru CTVM adota os seguintes controles adicionais de segurança cibernética:
(i) Perfis de configuração segura de ativos de tecnologia da informação: a Guru CTVM adota e mantém perfis de configuração segura (hardening) para todos os ativos de TI,

incluindo servidores, estações de trabalho, dispositivos de rede e sistemas em nuvem. Esses perfis definem parâmetros mínimos de segurança, desabilitam serviços e portas desnecessários e são revisados periodicamente pelo Diretor de Tecnologia e Segurança Cibernética.

(ii) Mecanismos de proteção da rede: a Guru CTVM implementa e mantém mecanismos de proteção da rede, incluindo segmentação de ambientes críticos, sistemas de detecção e prevenção de intrusão (IDS/IPS), firewalls de próxima geração e monitoramento contínuo do tráfego. Ambientes relacionados a sistemas de liquidação e custódia são isolados logicamente dos demais.

(iii) Gestão de certificados digitais: a Guru CTVM mantém processo estruturado de gestão do ciclo de vida de certificados digitais, abrangendo emissão, renovação, revogação e armazenamento seguro. O controle de validade dos certificados é monitorado de forma automatizada, evitando expirações não planejadas que possam comprometer a continuidade operacional ou a integridade das comunicações.

(iv) Requisitos de segurança para integração de sistemas via interfaces eletrônicas: toda integração de sistemas por meio de interfaces eletrônicas (APIs, conectores com B3, clearing, custodiantes e demais contrapartes) obedece a requisitos mínimos de segurança, incluindo autenticação mútua, criptografia em trânsito, controle de acesso por escopo e registro de trilhas de auditoria. Novos projetos de integração são submetidos a análise de segurança pelo Diretor de Tecnologia e Segurança Cibernética antes da entrada em produção.

(v) Ações de inteligência no ambiente cibernético: a Guru CTVM realiza ou contrata o monitoramento periódico de informações de interesse institucional na internet, na Deep Web e na Dark Web, incluindo a identificação de credenciais vazadas, menções à instituição e sinais de preparação de ataques direcionados. Os resultados são reportados ao Comitê de Riscos e incorporados ao ciclo de gestão de vulnerabilidades previsto na seção 4.6.

A implementação efetiva dos controles previstos nesta seção está em curso, com conclusão prevista para 31/12/2026. O Diretor de Tecnologia e Segurança Cibernética é o responsável pelo acompanhamento e reporte à Diretoria Executiva.

5. Classificação das Informações

Toda Informação criada ou recebida deve ser classificada e protegida ao longo de todo o seu ciclo de vida. O ciclo de vida das Informações compreende sua criação ou coleta, manuseio, análise, armazenamento, transporte, compartilhamento e descarte.

5.1. Tipos de Informação

(i) **Informações estruturadas:** criadas, acessadas e mantidas em sistemas, tais como informações utilizadas no funcionamento do aplicativo e sistemas da Guru CTVM. Cabe ao Comitê de Riscos a classificação dos níveis de sigilo relacionados a perfis de acesso, transações, telas, relatórios e conjuntos de informações;

(ii) **Informações não estruturadas**: estão fora dos sistemas corporativos, mas estão armazenadas no ambiente de TI, tais como: e-mails, documentos gerados em editores de texto, apresentações, planilhas, documentos impressos ou manuscritos. Cabe ao Gestor da respectiva área e ao Colaborador responsável a guarda e a classificação dos níveis de sigilo relacionados aos relatórios, apresentações, planilhas, pastas, mensagens de e-mail, manuscritos e demais documentos em papel, de acordo com as recomendações desta Política.

5.2. Níveis de Sigilo

Abaixo segue a classificação das Informações de acordo com os níveis de sigilo recomendados (público, privado ou interno e confidencial). A classificação das Informações (nível de sigilo) é de responsabilidade da área que as gerou ou coletou.

Classificação	Descrição
Informação Pública	Informações já publicadas oficialmente ao público externo em geral. Pode ser disponibilizada sem restrições. O conhecimento dessa Informação por qualquer indivíduo não causa impactos aos objetivos da Guru CTVM.
Informação Privada ou Interna	Informações que podem ser de conhecimento geral dos Colaboradores da Guru, mas que não podem ser divulgadas a pessoas ou empresas externas.
Informação Confidencial	Informações comunicadas de forma controlada apenas a Colaboradores e externos com obrigação de confidencialidade que necessitem conhecê-las para o exercício de suas funções e atribuições, incluindo, sem limitação, dados e informações sensíveis, entre eles os dados cadastrais e demais informações que permitem a

Classificação	Descrição
	identificação de Clientes (Dados Pessoais), suas operações e posições de custódia. O uso indevido desse tipo de Informação pode acarretar impacto financeiro, operacional, reputacional ou perda de vantagem competitiva. Quando extraviadas ou indevidamente utilizadas, podem prejudicar gravemente os objetivos de negócio da Guru CTVM. O Gestor responsável deve indicar explicitamente quais cargos e/ou funções podem ter acesso a Informações Confidenciais, determinando, inclusive, as Informações dentro do escopo de acesso.

As Informações classificadas como “Confidenciais” devem ser acompanhadas por uma lista de pessoas autorizadas em que o proprietário das referidas Informações especifica os nomes e/ou funções das pessoas que têm direito de acesso às respectivas Informações. A mesma regra da lista de pessoas autorizadas aplica-se ao nível de sigilo “Informação Privada ou Interna”, se pessoas de fora da Guru tiverem acesso a tais Informações.

6. RESPONSABILIDADES

A Guru CTVM mantém estrutura compatível com a natureza da instituição e com o perfil de seus clientes e usuários, bem como demais políticas instituídas. Nesse sentido, as atribuições são distribuídas da seguinte forma:

6.1. Diretor de Tecnologia e Segurança Cibernética

É o responsável por estabelecer, por meio da definição de políticas, padrões, procedimentos e Controles, a integridade, disponibilidade e a confidencialidade das Informações contidas nos ambientes da Guru CTVM, minimizando possíveis impactos e vulnerabilidades e reduzindo a ocorrência de Incidentes de Segurança que afetem os negócios da Guru CTVM, além de ser responsável por entender, gerenciar, reportar e escalar o Risco de Segurança Cibernética em sua área (incluindo ativos relevantes, informações, sistemas e terceiros); estabelecer e supervisionar a correta aplicação da estratégia de Segurança Cibernética em linha com os requisitos regulatórios; respaldar as áreas de negócio para impulsionar os comportamentos corretos de Segurança Cibernética; realizar avaliações de segurança e impor correções para os Riscos e vulnerabilidades de Segurança Cibernética; gerir atividades de proteção contra fraude eletrônica; e colaborar, coordenar e comunicar eventos de Segurança Cibernética com as áreas de negócio, reguladores, agências públicas e qualquer outro terceiro.

Desta forma, tem as principais atribuições:

(i) Governança e gestão de políticas de Segurança da Informação;
(ii) Gestão de acessos (definição de regras e critérios) e segregação de funções;
(iii) Certificação de Controles internos de Segurança Cibernética;
(iv) Definição de requisitos e análise de segurança em projetos, produtos e serviços;
(v) Gestão e detecção de vulnerabilidades;
(vi) Testes de invasão;
(vii) Busca e antecipação de ameaças e ataques cibernéticos;
(viii) Resposta a Incidentes de Segurança; e
(ix) Segurança de aplicações.

6.2. Gestores

Gestores são responsáveis por (i) conhecer, gerir e escalar o Risco cibernético de suas áreas; respaldar e permitir a adoção de defesas globais nos sistemas de Informação de suas áreas; proteger os sistemas e a Informação de suas áreas de acordo com os requisitos relevantes de Segurança Cibernética da Guru CTVM; e (ii) impulsionar os comportamentos corretos de Segurança Cibernética em suas áreas.

6.3. Colaboradores

Por fim, todo Colaborador deve observar e seguir as políticas, padrões e procedimentos estabelecidos pela Guru CTVM, sendo imprescindível a compreensão do papel da Segurança Cibernética em suas atividades diárias. Ainda, é de responsabilidade de cada Colaborador todo prejuízo ou dano que vier a sofrer ou causar à Guru CTVM ou a terceiros, em decorrência da não obediência às políticas aqui referidas e, caso seja desligado da Guru CTVM ou tenha seu contrato rescindido, deverá devolver todas as Informações da Guru CTVM que estiverem eventualmente em seu poder em razão dos serviços prestados.

6.4. Diretoria Executiva

A Diretoria Executiva da Guru CTVM deve gerir o Risco de Segurança Cibernética em linha com a governança corporativa da Guru CTVM, e com os requisitos regulatórios. Dessa forma, seus objetivos principais quanto ao tema são:

(i) apoiar as diretrizes desta Política, de forma a ser possível sua operacionalização no ambiente da Guru;

(ii) apoiar a cultura de Segurança da Informação e de Segurança Cibernética por meio de conscientização e treinamento para todos os Colaboradores;

(iii) apoiar e acompanhar as ações relacionadas à continuidade do negócio;

(iv) garantir os recursos necessários para a implantação dos Controles de Segurança da Informação e de Segurança Cibernética, conforme necessidades do negócio; e

(v) avaliar criticamente esta Política periodicamente.

6.5. Comitê de Riscos

O Comitê de Riscos tem a função de gerir e controlar a Segurança Cibernética. Dessa forma, seus objetivos principais quanto ao tema são: (i) supervisionar a posição e adequada gestão de Risco de Segurança Cibernética; (ii) revisar as vulnerabilidades e Incidentes de Segurança significativos, aprovar planos e programas de correção e preparar o relatório anual; e (iii) gerir e supervisionar o perfil de risco de Segurança Cibernética em linha com a estratégia e apetite de Risco definidos pela Guru CTVM.

7. Plano de Ação e Resposta a Incidentes de Segurança

O registro e a análise dos efeitos de Incidentes de Segurança relevantes são atividades cruciais para minimizar impactos negativos para a Guru CTVM. A equipe de TI deve estabelecer procedimento que possibilite a detecção tempestiva e a pronta comunicação de Incidentes de Segurança e vulnerabilidades.

O mapeamento de possíveis ataques é identificado por meio de Controles de detecção, que são implementados no ambiente. Os Controles contam com filtro de conteúdo, ferramenta de detecção de comportamentos maliciosos, antivírus e antispam, e outras ferramentas relevantes. É imprescindível que os incidentes identificados sigam sempre o processo de resposta a incidentes e que sejam comunicados ao Comitê de Riscos.

Na tentativa de prevenir vazamento de Informações, será feita a utilização de Controles, tendo como objetivo garantir que dados confidenciais não sejam mal utilizados, perdidos, roubados ou até mesmo vazados na web por usuários não autorizados.

Para detecção de anomalias nos sistemas de Informação, devem ser utilizadas tecnologias com ferramentas para detecção do tráfego anômalo, com objetivo de filtrar falsos positivos e bloquear eventos suspeitos, como *scrappers* (tentativa de extração de dados) e scanners (tentativa de buscar informações). Devem ser implementadas soluções que permitam bloquear automaticamente Incidentes de Segurança, como ataques DoS e/ou DDoS (ataques de negação de serviço). Podem também ser utilizadas soluções desenvolvidas internamente com o objetivo de detectar automaticamente o comportamento anômalo de

tráfego externo em aplicações internas.

Ainda, para garantir a segurança da Guru CTVM, conforme explicado acima, anualmente, deverão ser realizadas simulações de Incidentes de Segurança, incluindo testes de intrusão interno e externo nas camadas de rede e aplicação, bem como varreduras das redes, tanto internas quanto externas, devem ser executadas periodicamente. As vulnerabilidades identificadas deverão ser tratadas, sempre priorizando, sem limitação, as mais críticas.

7.1. Gerenciamento de Incidentes de Segurança

O gerenciamento de Incidentes de Segurança, que tem um papel fundamental para a manutenção dos negócios, é um processo por meio do qual a Guru CTVM reagirá a um incidente inesperado, que pode prejudicar sua imagem ou causar outros prejuízos. Também faz parte desse conjunto de práticas investigar possíveis Riscos e gerenciá-los antes que a crise se instaure. Esse gerenciamento tem como objetivo mitigar, reduzir ou excluir (se possível), os impactos causados por determinado momento de desequilíbrio, para que, assim, a empresa tenha o mínimo de prejuízo possível, sejam eles referentes à sua imagem ou financeiros. Dessa forma, a organização cibernética atua para desenvolver o plano de Controle da crise.

O grupo de gerenciamento de crise tem como fundamentos oferecer à Guru CTVM: (i) a capacidade de identificar, detectar e proteger, em todo o ambiente cibernético, os ataques cibernéticos que possam gerar um Incidente de Segurança Cibernética; (ii) a capacidade de responder rapidamente a ameaças que possam colocar em Risco a Guru CTVM, afetando a confidencialidade, a disponibilidade e a integridade dos ativos e informações tecnológicas; e (iii) garantir a eficácia da Segurança Cibernética. É necessário implementar procedimentos de governança que definem os atores, as responsabilidades e a categorização de incidentes para Informação e tratamento.

Nesse sentido, o grupo de gerenciamento de crise em conjunto com o Diretor de Tecnologia e Segurança Cibernética deve analisar os eventos relatados, decidir se eles devem ser classificados como Incidentes de Segurança da Informação ou não, e avaliar o nível de criticidade. O critério de avaliação do nível de criticidade deve ser estabelecido de acordo com o nível de exposição dos dados e pelo impacto para a continuidade dos negócios para a Guru CTVM e, dependendo da classificação, medidas devem ser tomadas considerando o

tempo de reação/solução.

A primeira comunicação deve ser feita diretamente ao grupo de gerenciamento de crise via e-mail ou outro meio rápido de contato, que assegure que as Informações cheguem ao responsável pela segurança corporativa. Todas as Informações necessárias para a análise (logs e outras Informações adicionais) devem ser enviadas na comunicação do evento. Deve ser levado em consideração que, como se trata de Informações confidenciais, essas Informações precisam ser protegidas contra acesso não autorizado e somente habilitadas ao grupo de pessoas que precisam dessas Informações.

Depois de receber as Informações de um evento de segurança, o grupo e a pessoa responsável pela segurança local ou a pessoa designada como tal, é responsável pela sua avaliação imediata, quando o evento começa, e toma a ação apropriada de acordo com os tempos de reatividade definidos pela criticidade do incidente.

7.1.1. Gerenciamento de Incidentes de Segurança Envolvendo Dados Pessoais

A Lei Geral de Proteção de Dados - LGPD estabelece normas sobre reação a Incidentes de Segurança Envolvendo Dados Pessoais, que são definidos como quaisquer acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito de Dados Pessoais.

Em qualquer uma das hipóteses abaixo, em que Dados Pessoais (isto é, dados referentes a pessoas naturais) tenham sido atingidos ou possam ter sido atingidos, é necessário comunicar o mais rápido possível ao Encarregado.

(i) Revelação de informações sensíveis;
(ii) Modificações indevidas de dados e programas;
(iii) Perda de dados e programas;
(iv) Perda, roubo ou extravio de dispositivos (laptops, smartphones, tablets e similares);
(v) Ataques, subversão, acidentes; e
(vi) Quaisquer outras falhas ou desvios das regras estabelecidas neste documento, bem como qualquer violação a elas, praticada em atividades relacionadas ao trabalho, dentro ou fora das dependências da Guru CTVM.

Uma vez identificado o incidente e mensurado o seu impacto, deve-se adotar medidas técnicas para reverter ou mitigar os efeitos deles decorrentes. Além disso, a depender do incidente e do impacto gerado para os titulares de Dados Pessoais afetados, será necessário proceder à comunicação do incidente, para os titulares de Dados Pessoais afetados e para a Autoridade Nacional de Proteção de Dados - ANPD..

A comunicação, que deve ser enviada aos titulares afetados e à Autoridade Nacional de Proteção de Dados - ANPD, deve conter, no mínimo:

(i) A descrição da natureza dos Dados Pessoais afetados;
(ii) As informações sobre os titulares envolvidos;
(iii) A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
(iv) Os Riscos relacionados ao incidente;
(v) Os motivos da demora, no caso de a comunicação não ter sido imediata; e
(vi) As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Assim, em caso de qualquer incidente, é relevante manter registros sobre tais informações.

No processo de gerenciamento de Incidentes de Segurança deve ser elaborado Plano de Ação e de Resposta a Incidentes definindo diretrizes quanto aos cenários, papéis e responsabilidades para comunicação e escalonamento.

Devem ser implementados Controles que permitam validar a implementação do processo de gerenciamento de Incidentes de Segurança e aplicar métricas para melhoria contínua.

Eventos de segurança devem ser classificados como um Incidente de Segurança Cibernética e/ou um Incidente de Segurança Envolvendo Dados Pessoais.

A identificação de Incidentes de Segurança pode ocasionar o bloqueio imediato dos acessos dos Colaboradores envolvidos até que sejam concluídas as investigações necessárias.

7.2. Plano de Ação e Resposta a Incidentes de Segurança

Ao ser identificado um Incidente de Segurança, devem ser seguidas as diretrizes contidas no Plano de Ação e Resposta a Incidentes de Segurança com o objetivo de minimizar a possibilidade de nova ocorrência do Incidente de Segurança em questão. A elaboração e o acompanhamento do plano de ação são coordenados pelo Comitê de Riscos, que para cumprir tais atribuições contará com a participação dos seguintes membros, entre outros:

Membros do Comitê de Riscos por Departamento	Nome	Cargo	Telefone	E-mail
Diretor Jurídico, Compliance e Risco	Guilherme Marin	Diretor Jurídico, Compliance e Risco	(48) 9 96536523	guilherme.marin@guructvm.com.br
Diretor de Tecnologia e Segurança Cibernética e Encarregado	Weverton Cesar Peres Bernardes	Diretor de Tecnologia e Segurança Cibernética	(11) 9 4758-8847	tom.bernardes@guructvm.com.br

O Plano de Resposta a Incidentes de Segurança da Guru CTVM deve contemplar procedimentos para continuidade dos serviços, incluindo:

(i) O tratamento para mitigar os efeitos dos Incidentes de Segurança e da eventual interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados;

(ii) O prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos; e

(iii) Na hipótese de identificação de um Incidente de Segurança Envolvendo Dados Pessoais, o Comitê de Riscos, seguindo o determinado na Política de Resposta a Incidentes de Segurança Envolvendo Dados Pessoais, deverá realizar análise do Incidente de Segurança

para verificar a possibilidade de Riscos ou danos relevantes aos titulares de dados afetados e deverá realizar comunicação tempestiva à Autoridade Nacional de Proteção de Dados - ANPD e aos titulares afetados, sempre que o Incidente de Segurança puder resultar em Risco ou dano relevante aos titulares.

7.3. Classificação da Criticidade dos Incidentes de Segurança

Os Incidentes de Segurança relacionados à Segurança Cibernética e os Incidentes de Segurança Envolvendo Dados Pessoais devem ser classificados conforme fatores de criticidade.

Os níveis de criticidade dos incidentes são: Crítico (P1), Alto (P2), Médio (P3) e Baixo (P4), conforme definidos na tabela abaixo. Caso a classificação seja considerada relevante, ela será comunicada tempestivamente ao Banco Central em cumprimento da Resolução 85/2021 e demais reguladores e autorreguladores necessários, bem como serão informados os clientes da instituição.

Classificação dos Incidentes de Segurança
Crítico (P1) - incidentes que resultem em indisponibilidade total das plataformas de negociação, afetando diversos processos críticos da Guru CTVM
Alto (P2) - incidentes que resultem em indisponibilidade parcial das plataformas de negociação, afetando processos críticos da Guru CTVM
Médio (P3) - incidentes que resultem em indisponibilidade em sistemas satélites e algumas funcionalidades, afetando alguns processos críticos
Baixo (P4) - incidentes que resultem em indisponibilidade de sistemas internos

7.4. Comunicação de Incidentes de Segurança

Os Colaboradores devem comunicar imediatamente todos os Incidentes de Segurança e eventuais violações desta Política ao Comitê de Riscos, sejam eles confirmados ou suspeitos, pelo e-mail incidentes@guructvm.com.br.

7.5. Relatório de Plano de Ação e Resposta a Incidentes de Segurança

Conforme explicado acima, com periodicidade anual, a Guru CTVM deve realizar testes considerando cenários de indisponibilidades causadas por Incidentes de Segurança. Adicionalmente, o Comitê de Riscos elaborará anualmente um relatório sobre a implementação do Plano de Ação e Resposta a Incidentes de Segurança, o qual deverá abordar, no mínimo, os seguintes itens ("Relatório Anual"):

(i) a efetividade das ações desenvolvidas pela Guru CTVM para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes desta Política;

(ii) o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos Controles, dos testes e das tecnologias a serem utilizados na prevenção e na resposta a Incidentes de Segurança; e

(iii) os Incidentes de Segurança relevantes ocorridos no período.

O Relatório Anual deverá ser apresentado à Diretoria Executiva da Guru CTVM.

7.6. Prevenção de Ocorrência de Incidentes de Segurança em Prestadores de Serviços

Os procedimentos e Controles voltados à prevenção e ao tratamento de Incidentes de Segurança em relação aos Prestadores de Serviços devem ser previamente definidos nos respectivos contratos. A avaliação de Riscos de tais serviços deverá ser realizada pelo Comitê por meio de diligência previamente à contratação de tais serviços.

8. Formas de Informação e Notificação dos Clientes

As precauções a serem adotadas no uso das plataformas da Guru CTVM, bem como a

ocorrência de eventuais falhas nos sistemas, serão comunicadas aos clientes por meio de mensagens digitais, via e-mail, SMS, Whatsapp, outros apps de mensagens, notificações de *push* ou qualquer outro meio a ser definido pela Guru CTVM.

Em casos de falhas, o time de atendimento deverá ser notificado e se manter alerta para responder a eventuais questionamentos por meio dos canais de atendimento aos clientes.

9. Reportes e Dúvidas

Constitui responsabilidade de todos os Colaboradores e terceiros garantir o cumprimento desta Política. Indícios de descumprimento ou dúvidas acerca do cumprimento desta Política poderão ser reportados ao Comitê de Riscos da Guru CTVM pelo e-mail comite-riscos@guructvm.com.br.

A Guru CTVM não tolera qualquer retaliação contra qualquer pessoa, interna ou externa, que comunique de boa-fé uma violação ou suspeita de violação a esta Política ou ao Código de Ética e Conduta do Grupo Guru, sendo garantida a confidencialidade acerca da identidade de qualquer pessoa que comunicar eventual violação.

10. Medidas Disciplinares

Ao ingressarem na Guru CTVM, todos os Colaboradores e partes relacionadas garantem que leram e compreenderam todos os termos desta Política, inclusive com relação ao monitoramento de suas atividades, estando cientes de que seus dispositivos, como computadores e seus serviços, como e-mail corporativo, são monitorados.

As violações de segurança devem ser informadas ao Gestor imediato e, simultaneamente, à área de Segurança da Cibernética. Toda violação ou desvio às diretrizes desta Política e de outras derivadas da mesma, é investigado para determinação das medidas necessárias e sujeita os Colaboradores a ações disciplinares e trabalhistas, bem como os Prestadores de Serviços e outros parceiros de negócios, incluindo-se a rescisão de contratos e penas de responsabilidade civil e criminal na máxima extensão que a lei permitir.

Indícios de irregularidades no cumprimento das determinações desta Política serão alvo de investigação interna e devem ser comunicados imediatamente aos nossos canais de

denúncias da Guru CTVM.

11. Disposições Gerais

A presente Política foi aprovada pela Diretoria Executiva e pelo Comitê de Riscos e entra em vigor a partir da sua publicação.

O conteúdo desta Política será revisado, obrigatoriamente, uma vez ao ano, a fim de que sejam implementadas melhorias, se necessário. Além disso, esta Política pode ser alterada sempre que a Diretoria Executiva julgar necessário em virtude de alguma alteração de Controles e/ou de produtos/serviços ou quando houver alteração na legislação ou regulamentação aplicável. As alterações a esta Política deverão ser aprovadas pela Diretoria Executiva e pelo Comitê de Riscos.

O descumprimento desta Política pode ensejar a aplicação de medidas disciplinares ao infrator e àqueles que com ele colaborarem, sem prejuízo das sanções administrativas ou criminais, que também possam decorrer das atitudes de descumprimento.

Os Colaboradores que eventualmente forem considerados infratores estarão sujeitos às sanções disciplinares previstas no Código de Ética e Conduta do Grupo Guru e em outros documentos internos da Guru CTVM, sem prejuízo de a Guru CTVM adotar as medidas administrativas, civis e penais cabíveis, conforme o caso.

Os Prestadores de Serviços que eventualmente forem considerados infratores estarão sujeitos às sanções contratuais cabíveis, incluindo a imediata rescisão contratual, com aplicação das penalidades decorrentes da rescisão, sem prejuízo de ação indenizatória e outras providências legais cabíveis.

*****