Sistema de Controles Internos

Política de Segurança Cibernética

Ano 2026
Revisada em 07/01/2026.

Sumário

1. Objetivo

Este documento estabelece os procedimentos, controles e práticas que devem ser adotadas por todos os colaboradores, estagiários, membros da diretoria, membros do Departamento de TI (DTI) e fornecedores com acesso local ou remoto à rede corporativa da Geral Investimentos (GI), com o objetivo de reduzir a vulnerabilidade a incidentes relacionados à segurança cibernética.

2. Prevenção e detecção de intrusão e vazamento de informações

A seguir serão descritos os sistemas, restrições, controle de acesso e monitoramento visando a prevenção e detecção de intrusão e vazamento de informações:

2.1 Sistemas de proteção

A GI dispõe de sistema de Firewall com IDS e IPS (Sistemas de detecção e prevenção de intrusão) ativados. Os logs de tentativa de acesso são analisados pelo DTI a fim de verificar se alguma ação é necessária.

As portas USB e a função de gravação de CDs/DVDs das estações de trabalho são bloqueadas a fim de impedir a contaminação por software malicioso ou vazamento de dados através de pen drives ou qualquer outra mídia portátil.

O firewall também dispõe de ferramentas que permitem monitorar e registrar a navegação dos usuários a fim de detectar, rastrear e bloquear vazamentos de dados sigilosos;

A GI possui ferramenta de antivírus instalada em todas as estações de trabalho e servidores de rede com atualização no mínimo diária. Os logs de detecção e atualizações são analisados pelo DTI a fim de verificar se alguma ação é necessária.

2.2 Programa de prevenção a vazamento de dados (DLP)

A GI adota conjunto integrado de controles para prevenir a exfiltração de dados sensíveis, em atendimento ao inciso IV da Resolução CMN nº 5.274/2025:

- Monitoramento de e-mail corporativo via Gatefy, com notificação automática ao Diretor de Controles Internos ao detectar transmissão de dados sensíveis de clientes ou informações confidenciais.
- Controle de navegação web via Trellix, bloqueando armazenamento em nuvem não corporativo, compartilhamento de arquivos e webmail externo.
- Bloqueio físico de dispositivos removíveis (USB, CD/DVD) em todas as estações de trabalho.
- Restrição de acesso a serviços de e-mail, mensageria e armazenamento em nuvem não autorizados pela GI.

Todos os alertas gerados pelas ferramentas de DLP devem ser registrados em sistema de chamados, analisados pelo DTI e reportados ao Diretor de Controles Internos. Vazamento confirmado aciona o protocolo de incidente Muito Grave da seção 4.

2.3 Restrições de acessos aos usuários

Os usuários não possuem permissões para instalar softwares ou mudar configurações do sistema operacional de suas estações de trabalho a fim de minimizar a possibilidade de instalações de softwares maliciosos e no caso de um incidente, minimizar seu impacto.

Os acessos a serviços de e-mail, chat online ou mensageria que não sejam de propriedade da GI são bloqueados, assim como qualquer serviço de armazenamento na nuvem.

2.4 Controles de acesso e segmentação de rede

Os servidores estão segmentados em uma DMZ (segmento de rede protegido). O acesso a esse segmento de rede é controlado pelo firewall e suas regras de IDS/IPS a fim de proteger os servidores de possíveis infecções por softwares maliciosos nas estações.

O acesso às pastas compartilhadas na rede pelo servidor de arquivos é segmentado por setor a fim de minimizar a propagação de software malicioso entre os mesmos.

O controle de acesso à rede é feito por um servidor com “Active Directory” da Microsoft, que autentica os usuários através de login e senha. Os logs de login e logoff são armazenados por 5 (cinco) anos.

2.5 Monitoramento e gerenciamento

O DTI monitora e trata no mínimo semanalmente os eventos detectados em todas as ferramentas de segurança (Anti-vírus e Firewall), bem como a checagem do bom funcionamento das mesmas.

O DTI verifica no mínimo anualmente possíveis vulnerabilidades em todos os sistemas, procedimentos e controles de segurança da GI através de testes de ataque aos sistemas, bem como testes de conhecimento e/ou teste de “pishing” aos usuários.

A GI possui uma matriz de segregação definida e aprovada pela diretoria, segmentar o acesso aos sistemas aplicativos e à rede corporativa de acordo com esse documento.

O acesso remoto feito por colaboradores ou membros do DTI à rede corporativa, sistemas aplicativos ou bancos de dados deve ser aprovado pela diretoria.

O aceso remoto feito por fornecedores de sistemas deve ser monitorado pelo DTI e gravado no caso de alguma alteração.

2.6 Treinamento e avaliação periódica dos usuários

A GI fornece treinamento sobre a segurança cibernética anualmente aos usuários, com o objetivo de minimizar incidentes e diminuir a vulnerabilidade global da empresa.

São aplicados testes anuais aos usuários, onde é exigido um mínimo de 70% de acertos para a aprovação, em caso de reprovação o usuário terá que refazer o teste no prazo de 30 (trinta) dias. O teste é aplicado pelo DTI da GI.

Na admissão de novos colaboradores, o treinamento e o teste devem ser aplicados em, no máximo, 60 dias a partir da data de admissão.

2.7 Conscientização de clientes e usuários

A GI disponibiliza aos clientes e aos usuários no site um manual sobre precauções na utilização de produtos e serviços financeiros.

3. Classificação dos dados e das informações quanto à relevância

Os dados e as informações da GI são classificados conforme demonstrado no quadro a seguir:

Classificação	Descrição	Observação
Muito Crítico	Sistemas aplicativos, banco de dados, documentos impressos utilizados na operação ou liquidação de ordens de clientes; e gravação das ordens.	*Os sistemas que fazem parte destes itens estão disponíveis para os órgãos reguladores e autorreguladores na GI.*
Crítico	Sistemas aplicativos, banco de dados, documentos impressos utilizados na manutenção de dados cadastrais, prevenção à lavagem de dinheiro, suitability, gestão de clubes, gestão de fundos, autenticação de rede e consulta para clientes.	
Não crítico	Documentos de apoio.	

4. Classificação, registro e tratamento dos incidentes

Os incidentes são classificados e tratados conforme demonstrado no quadro a seguir:

Classificação	Descrição	Tratamento
Muito Grave	I. Incidente que cause a indisponibilidade de algum sistema classificado como "Muito Crítico". II. Vazamento de dados de clientes.	I. Registrar em sistemas de chamados; II. Avisar a diretoria; III. Instruir os usuários e clientes de como deverão dar continuidade aos negócios até a solução do incidente; IV. Instruir os usuários e clientes de como prevenir o agravamento da situação; V. No caso de não haver previsão de reestabelecimento em menos de 1 (uma) hora, o PCN deverá ser acionado; VI. Tratar o incidente; VII. Criar processo, rotina ou melhoria de ferramenta que previna o incidente; VIII. Caso haja vazamento de dados sigilosos, o DTI deverá informar a área de Controles Internos para que avise os órgãos competentes.
Grave	I. Incidente que cause a indisponibilidade de algum sistema classificado como "Crítico".	I. Registrar em sistemas de chamados; II. Avisar a diretoria; III. Avisar os usuários; IV. Tratar o incidente; V. Criar processo, rotina ou melhoria de ferramenta que previna o incidente.
Regular	I. Incidente que cause a indisponibilidade de algum sistema classificado como "Não Crítico". II. Tentativa de invasão, infecção ou vazamento de dados detectada e bloqueada pelos sistemas de proteção.	I. Registrar em sistemas de chamados; II. Tratar o incidente; III. Criar processo, rotina ou melhoria de ferramenta que previna o incidente.

5. Critérios de declaração de crise operacional

A GI declara estado de crise operacional quando um incidente cibernético ou de tecnologia da informação atingir um ou mais dos critérios objetivos abaixo.

5.1. Critérios por impacto operacional

Declara-se crise operacional por incidente de tecnologia quando ocorrer ao menos uma das situações abaixo:

Critério	Parâmetro Objetivo
Indisponibilidade de sistema Muito Crítico sem previsão de restabelecimento	Duração superior a 1 hora em horário de funcionamento do mercado
Indisponibilidade do sistema de recepção ou execução de ordens de clientes	Independentemente da duração, se ocorrer durante pregão
Falha generalizada de autenticação de rede ou de sistemas críticos	Impacto em 50% ou mais dos usuários internos, ou em qualquer usuário de sistema Muito Crítico
Indisponibilidade simultânea de múltiplos sistemas críticos	Dois ou mais sistemas Críticos indisponíveis ao mesmo tempo por mais de 2 horas
Comprometimento da infraestrutura de rede principal (LAN/WAN)	Perda de conectividade que impede a operação normal por mais de 30 minutos
Acionamento do Plano de Continuidade de Negócios (PCN)	O acionamento do PCN configura automaticamente declaração de crise

5.2 Critérios por incidente de segurança da informação

Declara-se crise operacional por incidente de segurança da informação quando ocorrer ao menos uma das situações abaixo:

Critério	Parâmetro Objetivo
Vazamento ou exfiltração confirmada de dados confidenciais de clientes	Qualquer volume; declaração imediata independentemente da quantidade de registros
Acesso não autorizado confirmado a sistemas Muito Críticos ou Críticos	Independentemente do volume de dados acessados
Ransomware ou malware com impacto confirmado em sistemas produtivos	A partir da confirmação da infecção ativa
Comprometimento de credenciais de administrador de sistemas críticos	Qualquer credencial com privilégio elevado (admin, root, DBA)
Ataque DDoS que cause indisponibilidade de sistema Muito Crítico	Duração superior a 30 minutos ou ocorrência durante pregão
Violação de integridade de dados de ordens, posições ou liquidações de clientes	Qualquer alteração não autorizada; declaração imediata

Incidente que exija notificação compulsória ao BCB ou à CVM	A obrigação de notificar o regulador configura automaticamente declaração de crise

5.3 Procedimentos de declaração e encerramento

Identificado qualquer dos critérios acima, o DTI deverá:

1. Notificar imediatamente o Diretor de Controles Internos e a diretoria;
2. Registrar o incidente em sistema de chamados com hora, descrição e critério que motivou a declaração;
3. Avaliar o acionamento do PCN conforme seção 6;
4. Iniciar o protocolo de tratamento correspondente à classificação do incidente (seção 4);
5. Comunicar clientes e órgãos reguladores quando aplicável (seção 17).

O encerramento da crise deve ser formalmente declarado pelo Diretor de Controles Internos após confirmação de restabelecimento pleno e ausência de risco residual ativo, registrando-se o evento em ata.

6. Testes de continuidade de negócios

Anualmente a GI efetua um teste de continuidade, onde são testados os sistemas necessários ao processo de liquidação das operações em aberto nos casos de indisponibilidade dos mesmos no site principal da GI. A descrição dos procedimentos e cenários está descrito no PCN da GI.

7. Controle de acesso aos dados dos sistemas críticos

Os sistemas bancos de dados são controlados pelo DTI da GI. Quando há a necessidade de acesso por um fornecedor externo o acesso é monitorado e gravado pelo DTI.

8. Testes de vulnerabilidade e intrusão

O DTI verifica, no mínimo anualmente, possíveis vulnerabilidades em todos os sistemas, procedimentos e controles de segurança da GI através de testes de ataque aos sistemas. Os testes devem:

- Cobrir, no mínimo, os sistemas classificados como Muito Crítico e Crítico, a infraestrutura de rede e os sistemas de acesso remoto;
- Resultar em relatório com vulnerabilidades identificadas, classificação por criticidade e plano de remediação com prazos;
- Ter seus resultados apresentados à diretoria e registrados em ata;

- Ter relatórios e evidências de remediação retidos por, no mínimo, 5 (cinco) anos.

As vulnerabilidades críticas identificadas devem ter plano de remediação iniciado em até 30 dias.

9. Rastreabilidade da informação

Os sistemas aplicativos utilizados na rede corporativa da GI possuem trilha de auditoria que permite identificar as ações dos usuários.

A rede corporativa da GI possui trilha de login/logoff dos usuários que identifica o computador de origem, o usuário, a data e a hora do ocorrido.

Os mecanismos de rastreabilidade abrangem o processamento ponta a ponta dos dados, com os seguintes períodos mínimos de retenção:

Tipo de Log	Retenção Mínima
Logs de acesso à rede e sistemas internos	5 anos
Logs e documentos de ordens e operações de clientes	5 anos ou prazo regulatório específico, o maior
Logs de segurança (Firewall, IDS/IPS, DLP)	5 anos
Registros de incidentes e decisões do DTI	5 anos

10. Manutenção de cópias de segurança dos dados e das informações

As cópias de segurança são armazenadas em um ambiente segregado da rede corporativa e são realizadas e enviadas diariamente para armazenagem em local externo às instalações principais, com acesso controlado e controles de combate a incêndio, no prazo de retenção estabelecido pela regulamentação vigente. Todas as informações sobre cópias de segurança estão descritos na Política de Backup da GI.

11. Diretrizes de autenticação

Todos os sistemas, bancos de dados, servidores e serviços de rede, utilizados na rede corporativa, além de sistemas disponibilizados para clientes interna ou externamente, têm autenticação que obedece às diretrizes de senhas estabelecidas na Política da Segurança da Informação da GI.

12. Diretrizes de criptografia

Qualquer acesso externo aos sistemas, seja para cliente, colaborador ou fornecedor, é disponibilizado em canal seguro e criptografado.

Todas as senhas de usuários são armazenadas de forma criptografadas.

13. Diretrizes para contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem

Qualquer fornecedor de serviços, sistemas, processamento ou armazenamento em nuvem para os serviços descritos como “Muito Críticos” na Política de Segurança Cibernética da GI, devem atender os seguintes critérios:

- ✓ Assegurar a segurança física dos data-centers onde estiverem armazenados os dados da GI;
- ✓ Disponibilizar acesso aos dados armazenados;
- ✓ Garantir a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados, ou disponibilizar ferramentas para que a GI possa gerenciar esses itens;
- ✓ Possuir certificações de segurança da informação emitida por entidades regulamentadas no Brasil ou exterior;
- ✓ Garantir o acesso aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;
- ✓ Disponibilizar ferramentas para o monitoramento dos serviços a serem prestados;
- ✓ Identificar e segregar os dados por meio de controles físicos ou lógicos ou disponibilizar ferramenta adequada para os mesmos;
- ✓ Garantir a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da instituição, de acordo com o serviço de computação em nuvem contratado. Exemplos: Iaas, Paas, Saas, etc.; e
- ✓ Nos casos de prestadores Saas (Software as a service) o mesmo deve adotar controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do software.

14. Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem

Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever:

- ✓ A indicação dos países e da região em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;

O acesso da instituição contratante a:

- Informações fornecidas pela empresa contratada, visando a verificar o cumprimento do disposto nos incisos I a III;
- Informações relativas às certificações e aos relatórios de auditoria especializada;
- Informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

✓ A obrigação de a empresa contratada notificar a instituição contratante sobre a subcontratação de serviços relevantes para a instituição;

✓ A permissão de acesso do BCB aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações;

✓ A adoção de medidas pela instituição contratante, em decorrência de determinação do BCB;

✓ A obrigação de a empresa contratada manter a instituição contratante permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor;

✓ Parágrafo único. O contrato mencionado no caput deve prever, para o caso da decretação de regime de resolução da instituição contratante pelo BCB:

- A obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso, citados no inciso VII do caput, que estejam em poder da empresa contratada;
- A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços, com pelo menos 30 (trinta) dias de antecedência da data prevista para a interrupção, observado que:

  a) A empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de 30 (trinta) dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução;

  b) A notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.

- ✓ A adoção de medidas de segurança para a transmissão e armazenamento dos dados;
- ✓ A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes;
- ✓ A obrigatoriedade, em caso de extinção do contrato, de:
  - Transferência dos dados ao novo prestador de serviços ou à instituição contratante; e
  - Exclusão dos dados pela empresa contratada substituída, após a transferência dos dados prevista na alínea "a" e a confirmação da integridade e da disponibilidade dos dados recebidos.

15. Descarte e manutenção segura de dados e equipamentos

Todos os documentos impressos com dados de clientes são fragmentados em equipamento apropriado antes de serem descartados.

As mídias que contenham dados de clientes, tais como: HDs, SSDs, pendrives, disquetes, cartões de memória, CDs, DVDs, etc., têm os dados apagados permanentemente através de ferramenta específica e na impossibilidade disso a mídia deverá ser destruída.

16. Comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados à segurança cibernética

A diretoria da GI se compromete com a melhoria contínua dos procedimentos relacionados com a segurança cibernética através de revisões anuais dos processos implantados e investimentos na manutenção e melhoria dos mesmos. O responsável por esta política será o Diretor de Controles Internos.

As revisões serão feitas em conjunto com o DTI da GI.

17. Comunicação ao BCB e a CVM sobre compartilhamento de informação sobre incidentes

A GI comunicará os incidentes “Muito Críticos” e a previsão de reestabelecimento no seu *website* (www.geralinvestimentos.com.br), através de um banner em destaque na página inicial, incluindo a divulgação de um endereço de e-mail e números de telefones para contato, este banner ficará disponível inclusive nas redes sociais oficiais da GI.

Além da divulgação supracitada, a GI comunicará também o BCB de acordo com o inciso III do artigo 20 da Resolução 4.893/21 e suas alterações e a CVM de acordo com o artigo 46 sobre os incidentes relevantes ocorridos.

O site e as redes sociais serão os meios utilizados em virtude de não estarem na infraestrutura local da GI.

A GI comunicará ao BCB os incidentes considerados “Muito Críticos”.

18. Avaliação periódica de ameaças e vulnerabilidade

O DTI avalia anualmente os riscos de situações de ameaças e vulnerabilidades internas e externas à rede, servidores, sistemas e dados hospedados localmente ou na nuvem, utilizando a planilha "Planilha-analise-de-ameacas-e-vulnerabilidades-cibernéticas.xlsx" que está armazenada na pasta do Controles Internos.

A análise ocorre da seguinte forma:

1. É checado se todos os ativos de TI utilizados na GI estão listados na planilha;
2. Considera-se possíveis novas ameaças e vulnerabilidades para cada ativo;
3. É feita a avaliação qualitativa das ameaças e vulnerabilidades, além de uma analise de: Impacto x Probabilidade para determinar o risco;
4. Determina-se o tratamento e seu respectivo prazo para cada ativo que tiver o risco avaliado como grave ou muito grave;
5. A diretoria aprova as decisões em ata.