# 33. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

## 33.1. INTRODUÇÃO

A COGEM estabelece sua Política de Segurança da Informação e Cibernética, como parte integrante do seu sistema de gestão corporativo, alinhada às boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações da organização ou sob sua responsabilidade.

A COGEM entende que a informação corporativa é um bem essencial para suas atividades e para resguardar a qualidade e garantia dos serviços ofertados a seus associados.

A COGEM compreende que a manipulação de sua informação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações corporativas.

## 33.2. OBJETIVOS

**a)** Esta política tem por propósito estabelecer diretrizes e normas de Segurança da Informação e Cibernética que permitam aos colaboradores da COGEM adotar padrões de comportamento seguro, adequados às metas e necessidades da COGEM;

**b)** Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança Cibernética;

**c)** Proteger as informações da gestão da Cooperativa e de seus associados, preservando a integridade, confidencialidade e disponibilidade das informações;

**d)** Assegurar a continuidade do negócio da Cooperativa em casos de incidentes;

**e)** Atender as especificações do Banco Central que trata de segurança cibernética;

**f)** Atender a todas as legislações que tratam de segurança da informação;

**g)** Prevenir, detectar e evitar possíveis incidentes, vulnerabilidades e sanções legais à instituição e seus empregados, associados e parceiros;

**h)** Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de associados ou qualquer outro impacto

negativo no negócio da COGEM como resultado de falhas de segurança.

## 33.3. ESCOPO

Esta política se aplica a todos os usuários da informação da COGEM, incluindo qualquer indivíduo ou organização que possui ou possuiu vínculo com a COGEM, tais como empregados, ex-empregados, prestadores de serviço, ex-prestadores de serviço, colaboradores, ex-colaboradores, que possuíram, possuem ou virão a possuir acesso às informações da COGEM e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura COGEM ou na infraestrutura de terceiros locada pela COGEM.

Esta política deve ser divulgada a todos os colaboradores da COGEM em linguagem compatível com as funções que desempenham e em proporção à sensibilidade das informações que utilizam em seu cotidiano e disposta de maneira que seu conteúdo possa ser consultado a qualquer momento e seja protegido contra alterações. O público geral deve ter acesso a um resumo da política de segurança da informação. O conteúdo deste resumo, acessível pelo público geral, deve ser autorizado pelo Conselho de administração.

Funcionários devem comunicar à área de Controles Internos de qualquer evento, imediatamente após constatado, que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da COGEM.

## 33.4. DIRETRIZES

### 33.4.1. É política da COGEM:

De acordo com o requerido pela Resolução CMN nº 4893/21, esta Política é compatível com:

**a)** o porte, o perfil de risco e o modelo de negócio da COGEM;

**b)** a natureza das operações e a complexidade dos produtos, serviços, atividades e processos da COGEM;

**c)** a sensibilidade dos dados e das informações sob responsabilidade da COGEM.

Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da

informação da COGEM sejam atingidos através da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas.
Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: empregados, terceiros contratados e, quando pertinente, o público geral.
Garantir a educação e a conscientização a empregados, terceiros contratados e, quando pertinente, a associados, sobre as práticas de segurança da informação adotadas pela COGEM.
Atender integralmente requisitos de segurança cibernéticas aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais.
Tratar integralmente incidentes de segurança, garantindo que eles sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicados às autoridades apropriadas.
Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres.
Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática anual de objetivos de segurança em todos os níveis da organização.

### 33.4.2. Cultura de segurança cibernética

A COGEM deve promover a disseminação dos objetivos, princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação e divulgação ao público sobre precauções na utilização dos serviços e produtos oferecidos com o objetivo de fortalecer sua cultura de segurança cibernética.
Os programas de conscientização serão realizados anualmente a todas as partes interessadas e autorizadas no formato de cursos e material descritivo. Esporadicamente serão enviados comunicados contendo dicas e recomendações sobre como adotar práticas seguras que garantam a segurança da informação e sobre como minimizar os riscos, evitando incidentes relacionados à segurança da informação.
Ao concluir o programa de conscientização, o participante deve responder um questionário que avaliará o nível de conhecimento adquirido nos temas de segurança da informação apresentados e obter pelo menos 75% de acertos. Caso o participante apresente nível inferior

ao determinado pela área de Controles Internos, ele deverá refazer o programa de conscientização em segurança da informação.
A área de Controles Internos, TI, RH, Marketing e a Gerência são os responsáveis por garantir a eficácia e a implementação do programa de conscientização em segurança da informação. Uma reunião de alinhamento será feita anualmente para propor ajustes e melhorias à cultura de segurança cibernética. O Conselho de Administração deverá aprovar as decisões tomadas durante esta reunião anual, mediante a assinatura da ata. O quórum deste encontro anual deverá ser compatível com o exigido no estatuto da COGEM.
A COGEM se obriga a divulgar e/ou compartilhar materiais sobre boas práticas em segurança da informação em seu site, acessível pelo público geral, ou qualquer outro meio de comunicação autorizado pelo Gerência.
A área de Controles Internos, Marketing e RH são responsáveis por garantir a frequência e a qualidade da divulgação destes materiais no veículo utilizado para tal.

### 33.4.3. Incidentes de segurança da informação

Todas as ocorrências que possam vir a ter impacto negativo sobre a confidencialidade, integridade ou disponibilidade dos ativos/serviços de informação ou recursos computacionais da COGEM serão caracterizadas como um incidente de segurança da informação, devendo as referidas ocorrências serem tratadas de maneira a minimizar qualquer tipo de impacto e recuperar a confidencialidade, a integridade e a disponibilidade dos itens afetados.
Incidentes de segurança devem ser priorizados com base na criticidade dos ativos/serviços de informação ou recursos computacionais afetados, combinada com a estimativa de impacto prevista. Para efeitos de classificação da criticidade do incidente da informação, deve-se utilizar as seguintes categorias:

**a)** Preventiva: Efeitos apresentados em testes de incidentes e continuidades dos negócios.
**b)** Alta: Efeitos negativos severos.
**c)** Extrema Urgência: Efeitos negativos extremos.

Todos os incidentes de segurança ou suspeitas, devem ser comunicados à empresa terceirizada responsável pela área de T.I. da Cooperativa através de e- mail e/ou telefone, imediatamente após detectados, para

serem adequadamente registrados, classificados, investigados, corrigidos e documentados.
A empresa terceirizada de TI deverá determinar a criticidade do incidente através da avaliação do comportamento, confidencialidade, segurança física dos ambientes de operação e processamento, utilização de software e hardware e trilha de auditoria. Quando pertinente, comunicar as partes interessadas como, por exemplo, a Diretoria.
Na ocorrência de um incidente, incluindo interrupção de serviços, de segurança da informação, a área de Controles Internos ou colaboradores formalmente designados por ela sob a forma de Time de Resposta a Incidentes, deverá tomar as providências cabíveis à tratativa do incidente com base no documento Plano de Resposta a Incidentes da COGEM.
Um Relatório de Incidente de Segurança da Informação (RISI) deve ser preenchido para cada incidente ocorrido.
Se aplicável, a COGEM pode solicitar dos prestadores de serviços, informações relacionadas ao serviço prestado e/ou ao incidente e estas devem ser inseridas no RISI.
A área de Controles Internos, T.I. e a Gerência são responsáveis por garantir o funcionamento do seu Plano de Resposta a Incidentes. O plano deve ser revisado e verificado periodicamente por testes ativos ou passivos.
A área de Controles Internos, T.I. e a Gerência são responsáveis por garantir que o pessoal designado para executar o Plano de Resposta a Incidentes esteja suficientemente ciente dos detalhes do Plano. Isso pode ser feito de várias maneiras, tais como: exercícios práticos, participação em testes e programas de conscientização.
Todo incidente de segurança, após solucionado e documentado, deverá ser utilizado como uma ocorrência no documento Cenários de Incidentes, em que deve constar, no mínimo as seguintes informações sobre o incidente: nome, descrição e questões específicas relacionadas, sendo que o tratamento do incidente deverá ser adicionado ao Plano de Resposta a Incidentes, caso ainda não conste neste, para o caso de o mesmo incidente tornar a ocorrer.
Sem prejuízo do direito de confidencialidade da COGEM e com aprovação da Gerência, linhas gerais dos incidentes devem ser divulgadas ao público geral através do site da COGEM. É responsabilidade da Gerência compartilhar com o Banco Central do Brasil as ocorrências de incidentes.

### 33.4.4. Compartilhamento de informações

Conforme o inciso VII, art. 3º, da Resolução CMN nº 4.893/2021, as cooperativas devem compartilhar as informações referentes as ocorrências de incidentes cibernéticos relevantes com o Banco Central do Brasil e com as demais cooperativas por meio da Federação Nacional das Cooperativas de Crédito (FNCC).

### 33.4.5. Classificação e rotulagem da Informação

A Gerência deve classificar as informações, definir os direitos de acesso e os critérios de geração da informação sob sua responsabilidade, bem como garantir a exatidão das informações.

Os Funcionários da COGEM poderão acessar as informações relativas às suas atividades enquanto estiverem no desempenho de suas funções. As divulgações não autorizadas ou acessos indevidos podem causar impactos institucionais.

As empresas prestadoras de serviços que possuem acesso às informações, aos sistemas e/ou ao ambiente da COGEM devem conter cláusulas em seus contratos de prestação de serviços que assegurem o cumprimento das regras de segurança da informação, bem como penalidades no caso de descumprimento.

A classificação da informação deverá ser realizada pela Gerência ou colaboradores designados por esta. Entretanto, a responsabilidade pela atribuição do nível de classificação permanece com a Gerência.

O manuseio da informação da COGEM deverá obedecer às regras definidas abaixo:

**a)** Toda informação classificada como pública pode ser transmitida, copiada, enviada (qualquer que seja o meio) acessada por qualquer pessoa. Sua divulgação não causa qualquer dano à instituição.

**b)** Toda informação classificada como de uso interno pode ser transmitida, copiada, enviada (qualquer que seja o meio), acessada somente por colaboradores da COGEM.

**c)** Toda informação classificada como confidencial pode ser transmitida, copiada, enviada (qualquer que seja o meio), acessada somente por pessoas autorizadas pela Gerência.

Depois de classificadas, as informações precisam ser rotuladas. Todos os e-mails e documentos existentes na COGEM devem descrever a qual classificação eles pertencem. O rótulo de um documento pode ser apresentado no seu cabeçalho.
Documentos de uso interno ou confidenciais em formato eletrônico devem ser armazenados em ambientes com acesso controlado por mecanismos de autenticação seguros para impedir o acesso às pessoas não autorizadas.
Anualmente deve ser realizada a reclassificação dos dados ou quando caso ocorra alguma alteração.

### 33.4.6. Rastreabilidade da informação

Todas as informações nos ativos/serviços de informação ou recursos computacionais da COGEM podem ser interceptadas, gravadas, lidas, copiadas, descriptografadas e divulgadas por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais, seja originada de sua rede interna e destinada a redes externas ou o contrário. Estas informações incluem dados sensíveis criptografados para cumprir as exigências de confidencialidade e de privacidade.
Os acessos a informações classificadas pela Gerência devem ser rastreáveis, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente o usuário responsável.
A área de Controles Internos, T.I. e a Gerência ficam responsáveis por garantir a rastreabilidade das informações, inclusive pela implementação de controles específicos voltados a este propósito.

### 33.4.7. Gestão de vulnerabilidades

A COGEM disponibiliza ferramentas para detecção e proteção dos seus ativos/serviços de informação e recursos computacionais, incluindo estações de trabalho de usuários e servidores corporativos, contra intrusão e ameaças e programas maliciosos tais como vírus, cavalos de Tróia, vermes, ferramentas de captura de tela e dados digitados, softwares de propaganda e similares.
Informações classificadas como confidencial em formato eletrônico devem ser armazenadas em ambientes com acesso controlado, por meio de mecanismos seguros de autenticação, e criptografia para impedir o acesso às pessoas não autorizadas e possíveis vazamentos de informações sigilosas.

A prevenção de ameaças e proteção do ambiente cibernético da COGEM é realizada através da adoção, implantação e melhoria contínua de testes e varreduras de vulnerabilidades.

**a)** Os testes e varreduras de vulnerabilidades devem ser realizados em todos os sistemas do ambiente cibernético da COGEM, incluindo sistemas contratados, desenvolvidos e/ou adquiridos de prestadores de serviços e desenvolvidos pela própria COGEM.

**b)** Os testes e varreduras de vulnerabilidades devem ser realizados anualmente, podendo ser executados por empresas terceirizadas mediante aprovação da área de Controles Internos, T.I. e Gerência.

**c)** Após todo teste e varredura de vulnerabilidade, caso tenham sido detectadas vulnerabilidades no sistema, as mesmas devem ser corrigidas, a fim de reduzir a chance de um incidente ocorrer, e um novo teste e varredura de vulnerabilidades deve ser feito.

**d)** Todo teste e varredura de vulnerabilidades deve ser documentado. Constituem artefatos de documentação obrigatórios: relatório gerado no teste e varredura de vulnerabilidades, relatório descrevendo correções realizadas no ambiente e relatório produzido após novo teste e varredura de vulnerabilidades, provando que as falhas foram corrigidas.

**e)** A prevenção e detecção de intrusão no ambiente cibernético da COGEM deve ser realizada através da análise de registros de tráfego da rede da COGEM.

**f)** A análise deve ser executada semestralmente ou em período inferior, podendo ser realizada por empresas terceirizadas mediante aprovação da área de Controles Internos, T.I. e Gerência.

Todo sistema ou informação relevante para a operação dos negócios da COGEM deve possuir cópia diária dos seus dados de produção para que, em eventual incidente de indisponibilidade de dados, seja possível recuperar ou minimizar os impactos nas operações da instituição.

A Internet cabeada estará disponível apenas para máquinas e equipamentos de propriedade da COGEM, com a finalidade restrita à realização de atividades inerentes ao desempenho de tarefas laborais dos colaboradores.
A Internet sem fio deverá ser segregada, garantindo o isolamento da rede interna da COGEM, com o objetivo de fornecer acesso a sistemas e dados internos apenas para os colaboradores desempenharem suas tarefas. Poderá haver outras redes com acesso apenas à Internet para disponibilizar a visitantes e usuários que não precisam/podem ter acesso aos dados internos. A definição de qual rede o usuário deverá ingressar ficará a cargo da área de Controles Internos e da Gerência após análise dos requisitos de acesso.

### 33.4.8. Gestão de acessos

Acesso Físico: A COGEM mantém acesso restrito através de controles físicos apropriados e proporcional à criticidade dos equipamentos a todas as áreas onde serão processadas ou armazenadas informações pertinentes à sua operação, mantendo controle de acesso a estes ambientes somente a pessoas autorizadas.
Acesso Lógico: Na COGEM é vedado a realização de cópia de dados ou informações para mídias de armazenamento externo que não estejam pré-aprovadas, exceto com autorização da área de Compliance e T.I..
A COGEM mantém controle do acesso aos dados e sistemas de modo a garantir que apenas pessoas autorizadas tenham acesso, e adota processos de aprovações de usuários e perfis mediante a aprovações pelos responsáveis e efetuando a devida formalização destas autorizações e sua guarda.
A COGEM utiliza-se de matriz de segregação de atividades, definindo perfis de acessos e considerando as criticidades implícitas de cada permissão e função executada, dirimindo o risco de permitir conflitos de interesse e, realizando aprovações em alto nível para eventuais exceções. Periodicamente é realizada a revisão destes acessos concedidos e vigentes e ajustado em razão de identificação de riscos e/ou de mudança de função.

**a)** Acesso Remoto: O acesso remoto aos recursos computacionais é realizado adotando mecanismos de segurança definidos para evitar ameaças à integridade e sigilo das informações e dos serviços.

**b)** Parâmetros de senha: O acesso ao ambiente tecnológico ocorrerá através de senhas de autenticação do usuário, que deverão ser pessoais e intransferíveis. Referidas senhas deverão satisfazer os seguintes requisitos de complexidade:

- Ter pelo menos 08 caracteres de comprimento;
- Expirar, no máximo, a cada 60 dias (exceto para usuários de sistemas);
- Serem bloqueadas após, no máximo, 03 tentativas sem sucesso;
- Desbloquear através de ação do administrador do sistema;
- Não repetir, ao menos, as últimas 03 senhas utilizadas;
- Armazenar as senhas de forma criptografada;
- Trocar obrigatoriamente a senha inicial;
- Conter caracteres de maiúsculos (A-Z), caracteres minúsculos (a-z), números (0-9) e caracteres especiais (ex.: !, $, #, %).

### 33.4.9. Critérios de criptografia

Na gestão de chaves criptográficas, a COGEM adota controles para proteção das chaves criptográficas utilizadas nos processos de comunicação envolvendo a transmissão de informações de clientes (dados e transações).

**a)** Geração

As chaves criptográficas são geradas através de métodos reconhecidos, seguros e aprovados, e possuem grau de complexidade para garantir que o processo criptográfico adotado não se torne vulnerável, e quando necessário, os componentes atribuem código que possibilita a validação da sua integridade.

**b)** Armazenamento:

Os componentes das chaves criptográficas são armazenados em ambiente sistêmico e seguro e com acesso lógico restrito, criptografados, e protegidos contra divulgação ou utilização indevida.

**c)** Transmissão

Os componentes somente são transmitidos para e através de ambientes seguros e que possuem equipamentos ou sistemas que autorizam o tráfego de informações e/ou que armazenam os

próprios componentes. Os responsáveis estão cientes do sigilo que deve ser aplicado no manuseio destes componentes das chaves criptográficas.

**d)** Aplicação

- Transmissão de Informações - a transmissão de informações de transações e de informações de clientes, trafegadas na Internet, são criptografadas.
- Comunicação criptografada - a comunicação com demais sistemas corporativos, componentes de infraestrutura e equipamentos de rede, adota padrões de criptografia robusto.
- Rede sem fio - as redes sem fio utilizam protocolos de criptografia de modo a minimizar o risco de exploração de vulnerabilidades.

### 33.4.10. Prevenção e detecção de intrusão

A COGEM possui mecanismos para detectar eventos que possam comprometer a segurança das informações. O monitoramento do ambiente que suporta a plataforma é realizado na modalidade 24 x 7.

Prevenção ao vazamento de dados

A COGEM adota controles específicos para garantir a rastreabilidade da informação de forma a garantir a segurança das informações sensíveis. Entende-se por informação sensível toda informação dos clientes (dados pessoais ou bancários).

Neste sentido executa a prevenção e detecção de invasão e vazamento de informações, incluindo mecanismos de rastreabilidade da informação:

**a)** Estações de Trabalho

A segurança em estações de trabalho tem por objetivo manter as estações de trabalho seguras, e há parâmetros de configurações e controles de segurança que são estabelecidos nas estações de trabalho:

- Inclusão da estação de trabalho no domínio de rede COGEM;
- Instalação de softwares de segurança obrigatórios;
- Adequação dos perfis administrativos, onde somente devem permanecer no grupo de administradores locais das

estações de trabalho os usuários vinculados aos administradores de rede e equipes de suporte.

**b)** Restrições quanto à Instalação de Software e Hardware

A COGEM adota procedimentos de tecnologia da informação com o objetivo de controlar instalações de software e hardware em estações de trabalho:

- Instalações e configurações de software e hardware devem ser obrigatoriamente realizadas apenas pelas equipes de suporte da COGEM;
- Qualquer software utilizado em equipamentos corporativos de propriedade da COGEM deve ser previamente homologado;
- Todos os dispositivos de hardware instalados em equipamentos de propriedade da COGEM devem ser previamente homologados;
- Somente equipes de suporte da COGEM podem ter acesso administrativo em estações de trabalho.

**c)** Atualizações de Software

Está estabelecido um processo periódico de atualizações (patches) de segurança em equipamentos corporativos de produção.

A COGEM adota um conjunto mínimo recomendado de tecnologias pertencente ao processo de gestão de patches de segurança e executa as atualizações periodicamente, mediante o recebimento das atualizações.

**d)** Segurança em Servidores e em Rede

- A autenticação de usuários e acesso a informações armazenadas ocorrem exclusivamente por meio de user-id´s administrativos, previamente nomeados e autorizados ao uso pela COGEM;
- Armazenamento através de pastas de compartilhamento de dados de usuários que são utilizadas apenas para armazenamento de documentos de trabalho;
- É vedado o acesso anônimo aos servidores de arquivos;
- Adoção de controles para garantir a segurança da informação na rede e a proteção dos serviços conectados contra acessos não autorizados;
- Adoção de controles de autenticação em nível de rede;

- Possui segregação de redes para proteção das informações e sistemas de informação;
- Adoção de Termos de Responsabilidade para o uso responsável de dispositivos e informações, de navegação em internet, do uso de e-mail, e outros dispositivos e informações que são disponibilizadas.

### 33.4.11. Antivírus

A COGEM adota a proteção contra códigos maliciosos que tem por objetivo proteger as informações e os recursos de armazenamento, processamento e transmissão da informação, através de controles de detecção, prevenção e recuperação para proteção contra estes códigos.
São considerados códigos maliciosos: vírus, worms, trojans, spywares, adwares, ransomwares, keyloggers, exploits e demais códigos de natureza maliciosa.
O sistema de proteção contra malware é atualizado periodicamente e consulta bases de dados especializadas em reputação.

### 33.4.12. Uso da Internet

O acesso à Internet será autorizado para os usuários conforme a necessidade para o desempenho de suas atividades na COGEM;
É vedada a instalação de programas provenientes da Internet nos computadores da empresa, sem expressa anuência da área de TI;
É vedada a visualização, transferência (downloads e/ou uploads), cópia ou qualquer outro tipo de acesso a sites:

- De conteúdo adulto;
- Que defendam ou incentivem atividades ilegais;
- Que propaguem ou incentivem preconceito ou discriminação;
- Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios da empresa;
- Que possibilitem a cópia e/ou distribuição de informações de nível Interno e/ou Confidencial; e
- Que permitam a transferência (downloads e/ou uploads) de arquivos e/ou programas ilegais.

O acesso a redes sociais será autorizado, mediante aprovação da área da Diretoria, exclusivamente para atividades relacionadas ao negócio da empresa.

### 33.4.13. Uso do correio eletrônico

É um instrumento de comunicação interna e externa cujo objetivo é o de viabilizar a execução das atividades e negócios da empresa. Referidas mensagens, quando intercambiadas, devem prezar pelo profissionalismo e ser elaboradas e enviadas de forma a não comprometer a imagem e nem os princípios éticos da COGEM

Seu uso é individual sendo o seu usuário responsável por toda e qualquer mensagem enviada pelo seu endereço.

A COGEM deve empreender os meios necessários para a prevenção da perda de dados através das ferramentas disponibilizadas, controlando o fluxo da informação, dados e arquivos por meio de correio eletrônico.

### 33.4.14. Gestão de backups

A COGEM realiza constantemente suas cópias de segurança que tem por objetivo proteger as informações contra a perda e indisponibilidade. Os detalhes estão mencionados no documento anexo Política de Backup.

### 33.4.15. Monitoramento de logs

A COGEM detém as informações dos registros de eventos (logs) e os mantém protegidos contra acesso não autorizado e de adulteração.

Os controles adotados permitem a gestão destes dados e protegem contra modificações não autorizadas às informações dos logs e problemas operacionais com os recursos dos registros (log), incluindo:

- Alterações dos tipos de mensagens que são gravadas;
- Ativação e desativação dos recursos de auditoria;
- Arquivos de registros (log) permitindo edições ou exclusões;
- Capacidade adequada de armazenamento de registros (logs).

### 33.4.16. Gerenciamento de riscos

Um plano de contingência e continuidade (documento Plano de Continuidade de Negócios) para os principais sistemas e serviços da COGEM deverá ser implantado e testado no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

**a)** O Plano de Continuidade de Negócios deverá abranger cenários de indisponibilidade dos sistemas e dos serviços fornecidos por prestadores de serviços, cenários de

incidentes e prazo para normalização das atividades da COGEM, registrados no documento Cenários de Incidentes.

**b)** Os testes do Plano de Continuidade de Negócios avaliarão a eficácia do Plano de Continuidade de Negócios. Os responsáveis pelos testes deverão avaliar, para cada cenário testado: o tempo de solução, os mecanismos, procedimentos e controles utilizados e o conhecimento dos envolvidos no plano. Finalizados os testes, um relatório contendo o escopo e os resultados destes testes e as mudanças necessárias deverá ser criado e entregue à área de Controles Internos e a Gerência.

**c)** Os testes do Plano de Continuidade de Negócios devem ser coordenados pela equipe de tecnologia em conjunto com a área de controles internos que definirão os testes.

**d)** Um plano de resposta a incidentes (documento Plano de Resposta a Incidentes) deverá ser implantado e testado no mínimo anualmente, visando garantir que os incidentes em segurança da informação sejam devidamente tratados.

**e)** O Plano de Resposta a Incidentes deverá também abranger resposta a incidentes específicos, cujo comportamento já é conhecido (devido a incidentes semelhantes anteriores) e cujo fluxo de resposta deve atender as suas especificidades e ser registrados no documento Resposta a Incidentes.

**f)** Os testes do Plano de Resposta a Incidentes avaliarão a eficácia do Plano de Resposta a Incidentes, ou seja, se a COGEM possui recursos suficientes para responder a incidentes. Os responsáveis pelos testes deverão avaliar, para cada incidente testado: o tempo de solução, os mecanismos, procedimentos e controles utilizados e o conhecimento dos envolvidos no plano. Finalizados os testes, um relatório contendo o escopo, os resultados dos testes e as mudanças necessárias ao plano identificadas nos testes deverá ser criado e entregue à área de Controles Internos e a Gerência.

**g)** Os testes do Plano de Resposta a Incidentes devem ser coordenados pela área de Compliance da COGEM, que definirá o escopo destes.

A efetividade da política cibernética, do plano de ação e de resposta a incidentes e dos requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem deverá ser testada no mínimo anualmente, visando garantir que os procedimentos de segurança da informação adotados estão condizentes com o porte, o perfil de risco e o modelo de negócio da COGEM.

**a)** Os testes de efetividade avaliarão se todos os procedimentos de segurança da informação estão em conformidade com os requisitos da política de segurança da informação, do plano de ação e de resposta a incidentes e dos requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

**b)** Os testes de efetividade devem ser coordenados pela área de Compliance da COGEM, que definirá o escopo dos testes. Os responsáveis pelos testes deverão avaliar a adoção dos mecanismos, dos procedimentos e dos controles de segurança da informação e a existência de documentação comprobatória deles. Finalizado os testes, um relatório contendo o escopo dos testes e mudanças necessárias à política de segurança da informação, ao plano de ação e de resposta a incidentes e aos requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem deverá ser criado.

**c)** Se existirem prestadoras de serviços contratadas, estas devem cumprir os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem descritos no tópico "4.8. Prestadores de serviços" desta política, e a verificação do cumprimento deverá estar inclusa no escopo dos testes a serem realizados, certificando também a existência de subcontratações de serviços relevantes não notificadas.

**d)** As mudanças propostas a estes artefatos devem ser devidamente avaliadas e implementadas pela área de Controles Internos e pela Gerência anualmente ou, ainda, caso a área de Controles Internos e a Gerência avaliem que uma mudança proposta é prescindível, esta pode solicitar dispensa de implementá-la à Diretoria da COGEM. A Diretoria

da COGEM poderá conceder esta dispensa após uma reunião de mediação entre a área de Controles Internos, Gerência e a auditoria interna, responsável pela proposta de mudança.

### 33.4.17. Prestadores de serviços

Prestadores de serviços e/ou terceiros que manipulem, gerenciem, armazenem ou processem dados e informações da COGEM devem adotar procedimentos e mecanismos que garantam a segurança dos dados e da informação em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela COGEM. As decisões para a contratação de serviços relevantes de processamento de dados e de computação em nuvem atenderão requisitos e critérios objetivos, devidamente fundamentados, de modo que identifiquem e avaliem os riscos da contratação.

**a)** A COGEM garante que os procedimentos e mecanismos adotados pela prestadora de serviços cumprem os requisitos exigidos em legislações, regulamentações e políticas e normas internas da COGEM, bem como a documentação destes procedimentos e mecanismos.

**b)** Prestadoras de serviços que manipulem, gerenciem, armazenem ou processem dados e informações da COGEM devem, anualmente, contratar empresa de auditoria especializada visando avaliar os procedimentos e mecanismos utilizados nos serviços fornecidos. O relatório gerado deve estar à disposição da COGEM.

**c)** Prestadoras de serviços que manipulem, gerenciem, armazenem ou processem dados e informações da COGEM devem prover recursos de gestão adequados ao monitoramento dos serviços e informações solicitadas pela COGEM referente aos serviços contratados.

**d)** Prestadoras de serviços que manipulem, gerenciem, armazenem ou processem dados e informações da COGEM devem informá-la, assim que constatado, de todo incidente que ocorra no ambiente da prestadora de serviços que possa afetar o serviço prestado.

**e)** Os incidentes devem ser reportados, prevenidos, tratados e respondidos, tendo como referência o Plano de Resposta a

Incidentes da COGEM ou procedimentos estabelecidos durante a contratação.

**f)** Prestadoras de serviços que manipulem, gerenciem, armazenem ou processem dados e informações da COGEM devem garantir a confidencialidade, a integridade, a disponibilidade, a identificação, a segregação de demais clientes ao acesso aos dados e às informações pertencentes à COGEM.

**g)** Caso a prestadora de serviços subcontrate serviços de outra empresa e este faça parte do serviço fornecido à COGEM, a prestadora de serviços deve notificar a subcontratação.

**h)** Os sistemas contratados, desenvolvidos e/ou adquiridos que sejam mantidos por prestadores de serviços devem possuir mecanismos de prevenção e detecção de intrusão, estabelecidos durante a contratação.

**i)** Os mecanismos de prevenção e detecção de intrusão devem incluir testes e varreduras de vulnerabilidades realizados em todos os sistemas contratados pela COGEM.

**j)** Os testes e varreduras de vulnerabilidades devem ser realizados semestralmente ou conforme periodicidade estabelecida durante a contratação.

**k)** As correções às vulnerabilidades encontradas nos testes e varreduras de vulnerabilidades executados contra os sistemas da COGEM são de responsabilidade da empresa prestadora de serviços contratada.

### 33.4.18. Comunicações ao Banco Central

Serviços de processamento, armazenamento de dados e de computação em nuvem com nível de relevância ALTA devem ser comunicados pela COGEM ao Banco Central do Brasil.

A comunicação deve conter as seguintes informações e providências:

- A denominação da empresa a ser contratada;
- Os serviços relevantes a serem contratados;
- A indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;
- A comunicação da contratação dos serviços deve ser realizada 10 (dez) dias da contratação dos serviços;

- As alterações contratuais que impliquem modificação das informações relativas à contratação dos serviços, devem ser comunicadas ao Banco Central do Brasil, no mínimo, 60 (sessenta) dias antes da alteração contratual;
- A comunicação relativa à contratação dos serviços ou alteração contratual poderá ser realizada em prazo inferior a 60 (sessenta dias) em casos excepcionais, para garantir o regular funcionamento da COGEM e desde que acompanhada de justificativa fundamentada.

## 33.5. CASOS OMISSOS

Os casos omissos serão avaliados pela área de Controles Internos e pela Gerência para posterior deliberação.

As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação da COGEM adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações da COGEM.

## 33.6. REVISÕES

Esta política será revisada no mínimo anualmente.

## 33.7. GESTÃO DA POLÍTICA

A Política de Segurança da Informação e Cibernética deve ser aprovada pelo Conselho de Administração.