POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA TERCEIROS

GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO

Aos terceiros que se relacionam com o Sistema FIEMG,

A informação é um patrimônio de grande valor para o Sistema FIEMG e todos nós devemos zelar por ela, protegendo-a de forma a garantir sua confidencialidade, integridade e disponibilidade, conforme o Código de Conduta do Sistema FIEMG.

A tecnologia nos permite a obtenção, o armazenamento, o processamento e a recuperação de enormes quantidades de dados, essenciais aos fluxos administrativos e produtivos do Sistema FIEMG. O cuidado com estes dados, sua proteção e uso adequado, não só é parte integrante dos negócios, mas também do nosso diferencial competitivo.

O envolvimento e a adesão consciente de cada um de nossos terceiros, são fundamentais para consolidarmos o comportamento coletivo, mais atento e seguro, quanto ao tratamento das informações do Sistema FIEMG.

Contamos com a sua participação e compromisso quanto às diretrizes expostas a seguir.

SUMÁRIO

Histórico de versões

Versão	Data	Descrição	Autor(es)	Aprovador(es)
1.0	01/05/2021	Versão inicial	Carlos Eduardo Travagini Siqueira	Paulo Soares Ribeiro
1.1	27/08/2021	Revisão	Thaís Cristine dos Anjos Oliveira	Carlos Eduardo Travagini Siqueira
1.2	15/10/2021	Revisão	Thaís Cristine dos Anjos Oliveira	Carlos Eduardo Travagini Siqueira
1.3	22/07/2022	Revisão	Thaís Cristine dos Anjos Oliveira	Carlos Eduardo Travagini Siqueira
1.4	06/06/2023	Revisão	Thaís Cristine dos Anjos Oliveira	Rodrigo Fabiano da Silva Costa
1.5	29/11/2023	Revisão	Thaís Cristine dos Anjos Oliveira	Rodrigo Fabiano da Silva Costa
1.6	11/04/2024	Revisão	Suzy Santiago	Rodrigo Fabiano da Silva Costa
1.7	20/12/2024	Revisão	Suzy Santiago	Anderson Antônio Quintão Romero Bastos

1. INTRODUÇÃO

A Política de Segurança da Informação para Terceiros tem como objetivo definir as diretrizes que nortearão as normas e padrões que tratam da proteção da informação, abrangendo sua geração, utilização, armazenamento e compartilhamento, visando sua confidencialidade, disponibilidade e integridade, independentemente do meio e local em que ela esteja contida, com base na legislação vigente, órgãos reguladores e nas boas práticas de segurança da informação.

2. ABRANGÊNCIA

Esta Política se aplica a todos os parceiros de negócios que se relacionam com o Sistema FIEMG, como clientes, fornecedores, prestadores de serviços, contratados e outros, incluindo seus sócios, administradores, diretores, empregados, prepostos, contratados, consultores, ou quaisquer outras pessoas sob sua responsabilidade (direta ou indireta), que venham a ter acesso às suas informações corporativas e dados pessoais.

O cumprimento das diretrizes estabelecidas é fundamental para a efetiva relação de parceria firmada para atingir níveis adequados de proteção à informação.

3. VIGÊNCIA

Esta Política poderá ser revisada quando necessário, caso haja alguma mudança nas normas do Sistema FIEMG, alteração de diretrizes de segurança da informação, objetivos de negócio ou se requerido por órgãos reguladores.

4. DIRETRIZES

4.1. Uso da informação

Os terceiros tratarão de forma estritamente confidencial todas as informações corporativas e dados pessoais levados a seu conhecimento pelo Sistema FIEMG durante a prestação do(s) serviço(s) ou em função dele(s) e somente as utilizarão no âmbito dos serviços ora pactuados.

Todo terceiro deverá ter acesso somente às informações corporativas, dados pessoais e recursos que são necessários para a execução do seu trabalho.

Obrigam-se, portanto, a manter o sigilo e respeitar a confidencialidade de todas as informações corporativas e dados pessoais, verbais ou escritas, inovações, segredos comerciais, marcas, criações, especificações técnicas e comerciais do Sistema FIEMG, entre outros, a que tiverem acesso, conhecimento ou que venha a lhes ser confiado em razão da prestação do serviço, comprometendo-se, outrossim, a não revelar, reproduzir, utilizar ou dar conhecimento, em hipótese alguma e a qualquer tempo, bem como a não permitirem que nenhum de seus empregados faça uso desses dados, informações, materiais, inovações, segredos comerciais, marcas, criações, especificações técnicas e comerciais, entre outros, para fins alheios à prestação do serviço.

Os terceiros não estão autorizados a fornecer informações ou prestar declarações sobre assuntos internos do Sistema FIEMG, em qualquer mídia ou rede social, sobre os quais venham a ter conhecimento em razão do desempenho dos seus serviços contratados.

4.1.1. Proteção das informações

Todas as informações produzidas, individualmente ou em conjunto, pelos terceiros a serviço ou que se relacionam com o Sistema FIEMG, originadas ou derivadas de suas atividades de trabalho, são consideradas de nossa propriedade, aplicando-se, também, para qualquer informação provida ou licenciada pela organização.

Os terceiros deverão zelar e proteger as informações não públicas do Sistema FIEMG as quais possuem acesso; tais informações não podem ser divulgadas sem a prévia autorização do Sistema FIEMG. Não é permitido que se realize cópias dessas informações para uso pessoal ou de terceiros.

Os terceiros devem adotar medidas de segurança, técnicas e administrativas para proteger as informações e dados do Sistema FIEMG, utilizando de mecanismos, mas não se limitando, a criptografia, controle de acesso, mascaramento, dentre outros.

4.1.2. Proteção de Dados Pessoais

Os terceiros deverão conhecer a legislação aplicável à proteção de dados pessoais e à privacidade de seus titulares (Lei nº 13.709/2018 - LGPD), bem como dispor de meios necessários e suficientes à efetiva aplicação legal e para garantir o exercício dos direitos do

titular dos dados pessoais. Deverão adotar medidas de segurança, técnicas e administrativas para proteger os dados pessoais sob sua responsabilidade contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

4.1.3. Restrição de acesso à informação

O acesso às informações corporativas, dados pessoais e às funções de sistemas e aplicações são restritos de acordo com a Política de Controle de Acesso do Sistema FIEMG. Os requisitos abaixo são implementados pelo Sistema FIEMG, para conhecimento de todos os terceiros:

- Menus de controle de acesso às funções de sistemas e aplicações;
- Controle de dados que podem ser acessados pelos terceiros;
- Controle de direitos de acessos de terceiros, como leitura, exclusão, escrita e execução;
- Controle de direitos de acessos de terceiros a outras aplicações;
- Limitação de informações contidas nas saídas;
- Controles de acessos lógicos e físicos para proteção de dados pessoais, principalmente, dados sensíveis.

4.1.3.1 Acesso físico

Cabe às Gerências de Segurança Institucional, Segurança da Informação e Proteção de Dados, Logística e Administração e Meio Ambiente, estabelecerem as barreiras físicas necessárias para controlar o acesso e proteger as informações corporativas e dados pessoais da empresa. O terceiro deverá respeitar os acessos físicos a ele permitidos.

4.1.3.2 Locais sensíveis

Os terceiros devem respeitar as áreas e demais locais sinalizados como área de conteúdo sensível, cumprindo todas as definições e proibições de registros fotográficos, gravações de áudio, vídeo, bem como restrições de compartilhamento em qualquer mídia ou rede social.

4.1.4. Armazenamento de informações

Os terceiros devem informar ao Sistema FIEMG, quando solicitado, as medidas de segurança para a transmissão e armazenamento das informações corporativas e dados pessoais. Toda

informação processada e/ou armazenada pelo terceiro deve haver segregação de dados e dos controles de acesso, lógico e físico.

Devem haver rotinas sistemáticas de *backup*, cópias dos dados de produção, *backup* local e *backup off-site*, aplicando-se as melhores práticas de mercado com relação à segurança da informação e proteção de dados. As cópias de segurança devem ser armazenadas a uma distância suficiente para escapar dos danos de um eventual desastre, bem como as mídias de *backup* devem ser regularmente testadas para garantir que elas são confiáveis no caso do uso emergencial.

Documentos físicos devem ser arquivados de forma segura, seja em ambiente interno ou externo, contemplando barreiras físicas e proteção como trancas, biometria, dentre outros, e mantê-los guardados de acordo com os prazos previstos em lei.

A transmissão e armazenamento de informações em nuvem deverá ser realizada exclusivamente pela Microsoft OneDrive e Sharepoint corporativos.

4.1.5. Descarte da informação

Após o término da prestação de serviço, todas as informações corporativas e dados pessoais utilizados devem ser devolvidos ao Sistema FIEMG em, no máximo 30 (trinta) dias, devendo enviar um comprovante assinado por seu representante legal certificando tal devolução.

4.2. Uso dos recursos de tecnologia

Quando da utilização dos recursos de tecnologia fornecidos pelo Sistema FIEMG, não é permitido ao terceiro acessar, propagar, manter ou utilizar sites, aplicativos, redes sociais, e/ou conteúdo que, entre outros:

- Infrinjam qualquer lei e/ou regulamento local, estadual, nacional ou internacional aplicável;
- Ofendam os direitos à honra, à vida privada, à imagem, à intimidade pessoal e familiar de quem quer que seja, ou à própria imagem das pessoas, assim como a propriedade intelectual;

- Incitem e/ou promovam ações ou ideias discriminatórias em razão de raça, gênero, orientação sexual, religião, crença, deficiência, etnia, nacionalidade ou condição social;
- Constituam comportamento predatório, perseguição, ameaças, assédios, intimidações ou chantagem a terceiros;
- Contenham material obsceno, pornográfico, impróprio, ofensivo, violentos e/ou que estimulem a prática de condutas contrárias à moral e aos bons costumes e/ou criminosas, perigosas, de risco ou nocivas à saúde;
- Incitem práticas perigosas, de risco ou nocivas à saúde e ao equilíbrio psíquico;
- Violem direitos autorais ou estimulem a pirataria e/ou utilizem conteúdo ou material cujo direito pertença a terceiros, sem ter um contrato de licenciamento ou outros tipos de licença;
- Violem segredos empresariais de terceiros;
- Façam apologia a crimes;
- Constituam publicidade ilícita, enganosa ou desleal, que configurem concorrência denominados "*spam-mail*", ou, ainda, correspondência corporativa e comunicações com finalidade comercial (prospecção de negócios, venda de serviços e mercadorias, ainda que relacionados à pessoa física, etc.) ou uso relacionado com negócios, ou que anuncie ou ofereça a venda de produtos ou serviços (com ou sem fins lucrativos) ou que solicitem outros usuários ou terceiros (incluindo pedidos para contribuições ou donativos);
- Efetuem ou tentem efetuar qualquer tipo de acesso não autorizado aos recursos computacionais do Sistema FIEMG ou de terceiros ("*Hacking*"), tais como invasões, alterações ou destruições de recursos computacionais; e
- Introduzam qualquer forma de vírus de computador, *malware* ou qualquer outro elemento nocivo ou danoso dentro do ambiente de tecnologia do Sistema FIEMG ou de terceiros.

É vedada, ainda, a realização de atividades não contratadas e/ou a atuação de forma negligente e imprudente, que possa resultar em avarias ou impedir o normal funcionamento da rede, dos sistemas ou dos equipamentos (*hardware e software*) do Sistema FIEMG, ou que possam danificar ou corromper informações corporativas, dados pessoais e documentos eletrônicos.

4.2.1. Fornecimento de recursos ou dispositivos corporativos

Somente será disponibilizado ao terceiro recurso ou dispositivo corporativo, tal como acesso a sistemas, rede cabeada, correio eletrônico, entre outros, em caso de necessidade para o acesso seguro às informações e ambiente interno de tecnologia.

Ao utilizar algum recurso ou dispositivo corporativo, cabe ao terceiro conhecer e aplicar todas as políticas, normas e manuais internos que regem a sua utilização, bem como zelar pela proteção física e integridade dos dispositivos cedidos, visando a preservar as informações corporativas e dados pessoais do Sistema FIEMG.

4.2.2. Uso de dispositivos móveis

Mediante solicitação prévia o Sistema FIEMG tem a faculdade de autorizar o uso de dispositivos móveis de propriedade de terceiros para a execução da prestação do serviço ora pactuado. Nesse caso, a compatibilidade dos dispositivos móveis e as demais configurações necessárias para uso no ambiente interno da Entidade é de responsabilidade do terceiro.

O Sistema FIEMG não fornece aplicativos, atualização de sistemas ou soluções de tecnologia para dispositivos móveis de propriedade de terceiros, limitando-se a orientar os terceiros, na hipótese de ser necessário o uso dos mesmos.
O Sistema FIEMG poderá, no entanto, orientar a aquisição ou fornecer aplicativos específicos necessários para o acesso seguro às informações corporativas e dados pessoais em alguns ambientes de tecnologia.

4.2.2.1 Controle de acesso

Os dispositivos móveis de propriedade de terceiros usados nas instalações do Sistema FIEMG devem ser protegidos por senha pessoal ou controles que impeçam o acesso não autorizado. Cada terceiro é responsável pela proteção de seus dispositivos contendo informações corporativas e dados pessoais que estão sob sua guarda.

O acesso lógico ao ambiente da rede interna do Sistema FIEMG será avaliado e aprovado de acordo com a necessidade, seguindo a Política de Segurança da Informação.

Quando aplicável, o usuário e senha disponibilizados para o terceiro são de uso exclusivo e não podem ser divulgados ou compartilhados, devendo seguir todas as políticas, normas e procedimentos internos do Sistema FIEMG que lhe forem informados. Suas credenciais de acesso devem ser mantidas em segurança e qualquer uso indevido são de sua responsabilidade.

A empresa terceira deverá comunicar qualquer desligamento de terceirizados para que os mesmos tenham seus acessos devidamente cancelados no ambiente do Sistema FIEMG.

4.2.2.2 Senhas de acesso

Devem ser criadas senhas seguras para acesso aos dispositivos utilizados no âmbito da prestação do serviço ao Sistema FIEMG, independentemente se o equipamento é de propriedade particular ou do Sistema FIEMG. Recomendamos as seguintes boas práticas:

- Criar senhas fortes e com complexidade, contemplando, no mínimo, 8 caracteres, letras maiúsculas e minúsculas, números e caracteres especiais;
- Jamais compartilhar senhas, seja verbalmente, por escrito ou eletronicamente, etc.;
- Ativar a autenticação multifatorial MFA em todas as aplicações que fornecem esse recurso;
- As senhas devem ser alteradas sempre que houver qualquer indicação de que foram descobertas ou houve tentativa de força bruta. Neste caso, principalmente para equipamentos de propriedade do Sistema FIEMG disponibilizado ao terceiro, um incidente de segurança deve ser reportado à equipe de Segurança da Informação, por meio do email si@fiemg.com.br.

4.2.2.3 Proteção contra ameaças digitais

Os dispositivos móveis de propriedade de terceiros usados nas instalações do Sistema FIEMG ou conectados às suas redes devem possuir *softwares* de proteção contra ameaças digitais (p. ex. vírus, *malware, spyware*, trojans, entre outros).

Caso o terceiro identifique qualquer uma destas ameaças em seu dispositivo móvel ou em outro meio tecnológico utilizado nas dependências do Sistema FIEMG, deverá avisar imediatamente à equipe de Segurança da Informação através do e-mail si@fiemg.com.br.

4.2.2.4 Atualização do dispositivo móvel

Os usuários de dispositivos móveis de propriedade de terceiros deverão obrigatoriamente manter atualizados seus sistemas e aplicativos conforme dados divulgados pelos fabricantes, visando minimizar a existência de falhas de segurança ou vulnerabilidades. As atualizações são de inteira responsabilidade do terceiro.

4.2.2.5 Auditoria e conformidade

Fica a critério do Sistema FIEMG fiscalizar, mediante aviso prévio ao terceiro, os dispositivos móveis de propriedade de terceiros utilizados em suas dependências visando certificar que as diretrizes desta Política de Segurança da Informação estão aplicadas de forma adequada.

4.2.3. Uso de software

O uso de *software* não licenciado e/ou pirata é ilegal, expressamente vedado e será considerado como infração grave a esta Política, podendo resultar na rescisão dos contratos com os terceiros e aplicação de penalidades. Caso seja identificado o uso indevido de *software* ou aplicativo pelo terceiro, o Sistema FIEMG poderá impedir sua utilização, bem como tomar as medidas necessárias para evitar danos decorrentes do uso indevido, sem prejuízo da obrigação do terceiro em ressarcir todos e quaisquer ônus incorridos pelo Sistema FIEMG.

4.2.4. Rede cabeada, Wifi e Internet

Os terceiros deverão aceitar e seguir todas as políticas, normas e procedimentos internos do Sistema FIEMG que lhe forem informados para a utilização da rede cabeada, *wifi* e internet.

4.3. Controles de segurança no ambiente do terceiro

O terceiro que tratar (considerando e não se limitando a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração) as informações do Sistema FIEMG em seu ambiente, deve seguir as seguintes diretrizes de segurança da informação:

4.3.1. Controle de acesso

Possuir documentado um processo de gerenciamento de acessos e dar acesso irrestrito aos dados e informações armazenadas ou a serem processadas, conforme os serviços específicos

definidos, prezando pela confidencialidade, integridade, disponibilidade e pela capacidade de recuperação destes dados e informações.

4.3.2. Teletrabalho

Caso o terceiro execute as atividades no âmbito da prestação do serviço em teletrabalho, faz-se necessário a aprovação e autorização prévia pelo Sistema FIEMG. Dada a continuidade, o terceiro deve agir com máxima diligência, a fim de evitar que informações do Sistema FIEMG sejam acessíveis por estranhos ou pessoas não autorizadas, devendo observar, no mínimo, as recomendações abaixo.

4.3.2.1 Local de teletrabalho

Acesso remoto a sistemas, infraestrutura de suporte ao ambiente de tecnologia ou informações do Sistema FIEMG é precedido, obrigatoriamente, por um processo de autenticação do usuário, a qual deve seguir as regras definidas pela empresa, podendo conter 01 (um) ou mais fatores de autenticação, conforme a criticidade do sistema, ativo de tecnologia e/ou informação a ser acessada. Além disso, a realização de teletrabalho em áreas onde a privacidade não possa ser obtida, como aeroportos, salas de reunião, salas de espera, transportes públicos, restaurantes, entre outros, por meio da internet disponibilizada de forma gratuita, não deve ser realizada. Orientamos preferenciar o uso compartilhado por um dispositivo móvel de uso pessoal, que utiliza a tecnologia 4G ou 5G, visto a asseguridade do serviço de dados contratado pela operadora em uso.

4.3.2.2 Tráfego de informação

Todo o tráfego de informação realizado durante o teletrabalho deve ser controlado por medidas técnicas de segurança elevadas e adotadas pelo mercado.

4.3.2.3 Revogação do acesso

O acesso remoto será revogado ao término do contrato de prestação de serviço ou a qualquer tempo, devido ao regresso e/ou substituição do usuário prestador de serviço, a violação de políticas, normas e procedimentos vigentes, determinação do Comitê de Integridade e/ou necessidades do Sistema FIEMG.

4.3.2.4 Monitoramento

Os acessos realizados pelos terceiros durante a sessão de teletrabalho são registrados pelo Sistema FIEMG e podem ser fiscalizados, a qualquer momento, sem necessidade de aviso prévio. O Sistema FIEMG poderá, a qualquer momento, bloquear o acesso do equipamento à rede corporativa, caso sejam detectadas desconformidades com as políticas, normas e procedimentos vigentes.

4.3.3. Segurança no desenvolvimento de sistemas

Desenvolver sistemas levando em consideração os padrões de segurança aceitos pelo mercado e descrever os recursos de segurança e os dados acessados pelas aplicações, os quais devem ser avaliados pela equipe de Segurança de Informação durante a fase de homologação (Ex: especificação técnica e/ou diagrama funcional);

Utilizar rotinas de validação de integridade para prevenir erros, seja involuntário ou intencional e prever as validações de segurança no processo de qualidade e verificação de código. No mínimo, devem ser consideradas aquelas que constam no OWASP TOP 10.

4.3.4. Monitoramento dos serviços

Assegurar que dispõe do mais alto nível de capacidade no provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados, bem como garantir o cumprimento da legislação e da regulamentação em vigor, além de aderir todas as certificações exigidas pelo Sistema FIEMG para a execução dos serviços contratados.

4.3.5. Subcontratação de serviços

Notificar, de imediato, a necessidade de subcontratação de serviços relevantes para o Sistema FIEMG.

4.3.6. Mesa limpa e tela limpa

Sempre que estiver trabalhando com informações corporativas e dados pessoais do Sistema FIEMG, o terceiro deve garantir que nenhuma informação confidencial esteja disponível para outros terceiros. Recomendamos:

- Os documentos impressos não devem estar disponíveis na estação de trabalho ou em outros locais (impressoras, fotocopiadoras, etc.) sem a presença do responsável por tais documentos;
- Bloquear a tela de *desktops*, *notebooks* e/ou demais dispositivos durante a ausência do prestador do serviço, além de protegê-los com senha segura e autenticação de duplo fator;
- Documentos contendo informações corporativas e dados pessoais do Sistema FIEMG devem ser removidos imediatamente das impressoras e copiadoras.

4.3.7. Gestão de vulnerabilidade

Prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados ao ambiente cibernético, enviando os seus melhores esforços e usando de procedimentos e controles, que abranjam, no mínimo, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidade, a proteção contra *softwares* maliciosos, 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.

4.3.8. Gestão de incidentes

Possuir um processo estruturado de resposta a incidentes. Fornecer, quando solicitado, as informações relacionadas a quantidade de incidentes ocorridos no período de 12 meses, classificando-os pela sua relevância e manter o Sistema FIEMG permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

4.3.9. Continuidade de negócios

Definir um programa de continuidade de negócios, para assegurar que possíveis incidentes não afetem os serviços prestados ao Sistema FIEMG.

4.3.10. Certificações e auditorias independentes

Informar e dar acesso ao Sistema FIEMG, quando solicitado, sobre as certificações necessárias para a prestação dos serviços, bem como aos relatórios relacionados aos controles utilizados, elaborados por empresa de auditoria independente especializada.

4.3.11. Treinamento e conscientização

Os terceiros devem oferecer conscientização e treinamento periódico no âmbito da segurança da informação para seus empregados, parceiros, clientes e demais públicos, os quais possuirão acesso às informações corporativas e dados pessoais do Sistema FIEMG.

5. DISPOSIÇÕES FINAIS

5.1. Avaliações periódicas

O Sistema FIEMG poderá realizar, sempre que achar necessário, avaliações para atestar a efetividade da implementação dos controles apresentados nesta Política, devendo para isso, comunicar o parceiro com 30 dias de antecedência.

5.2. Situações especiais e exceções

As situações especiais e/ou pedidos de exceção a esta Política deverão ser avaliados pela Gerência de Segurança da Informação por meio do email si@fiemg.com.br.

Caso os terceiros ou quaisquer de seus representantes sejam obrigados, em virtude de lei, de decisão judicial ou por determinação de qualquer autoridade governamental, a divulgar quaisquer informações confidenciais, deverão comunicar imediatamente ao Sistema FIEMG, para que a empresa tome as medidas cabíveis, inclusive judiciais, para se preservar.

Na hipótese das medidas tomadas para preservar as informações confidenciais não terem êxito, a revelação aqui tratada estará limitada, tão somente, às informações que sejam legalmente exigíveis.

5.3. Casos omissos

Antes de efetuar ações que possam apresentar risco potencial para as informações corporativas e dados pessoais do Sistema FIEMG, o terceiro deve consultar as demais políticas, normas e manuais internos, caso aplicável, a fim de certificar-se de que a atividade é lícita e segura. Os casos não previstos ou dúvidas sobre segurança da informação deverão ser encaminhados para a equipe de Segurança da Informação do Sistema FIEMG, através dos canais de contato disponíveis.

5.4. Conformidade

As violações às disposições estabelecidas na presente política, devidamente apuradas, estarão sujeitas:

a) Ao imediato cancelamento do acesso às instalações do Sistema FIEMG;

b) À aplicação das sanções previstas no contrato de prestação de serviço;

c) Ao cancelamento ou rescisão do contrato;

d) À aplicação dos procedimentos legais cabíveis.

5.5. Documentos de referência

- Código de Conduta para terceiros do Sistema FIEMG
- Aviso de privacidade e proteção de dados do Sistema FIEMG
- Programa de Integridade do Sistema FIEMG
- Políticas, normas e manuais de segurança da informação do Sistema FIEMG;
- ABNT NBR ISO/IEC 27002 – Segurança da informação, segurança cibernética e proteção à privacidade – controles de segurança da informação.