SEGURANÇA DA INFORMAÇÃO

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 da 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. INTRODUÇÃO

A informação é um dos elementos mais importantes para o Sistema FIEMG e, dessa forma, manter a sua confidencialidade, integridade, disponibilidade e autenticidade são fatores críticos para o nosso negócio.

- Confidencialidade: Garantia que a informação estará acessível apenas para pessoas autorizadas;
- Integridade: Preservação dos dados, não sendo possível realizar qualquer alteração por pessoas não autorizadas;
- Disponibilidade: Garantia que os dados possam ser consultados a qualquer momento;
- Autenticidade: Garantia de que os dados possuem legitimidade, ou seja, não haja manipulação ou intervenções externas;

A Política de Segurança da Informação para terceiros tem como objetivo principal direcionar um programa efetivo de proteção dos ativos de informação, sendo a base para o estabelecimento de todos os padrões e procedimentos de segurança.

2. ABRANGÊNCIA

Esta política se aplica a todos os prestadores de serviços contratados pelo Sistema FIEMG, 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.

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. TERMOS E DEFINIÇÕES

- Terceiro: Prestador de serviço, parceiro de negócio, contratado ou fornecedor.
- Dispositivo móvel: *notebook*, *tablet*, *smartphone* ou qualquer outro dispositivo usado para acessar, produzir e/ou armazenar informações do Sistema FIEMG em qualquer lugar, dentro ou fora da empresa.
- Fator de autenticação: capacidade de provar que um usuário é realmente quem ele diz ser. Os fatores de autenticação podem ser compostos por algo que você sabe (p.ex.: senha de acesso), algo que você tem (p.ex.: *token*, crachá, chave, etc.) e/ou algo que você é (p.ex.: biometria).
- Teletrabalho: são todas as formas de trabalho fora do escritório e que vise a atender as necessidades do Sistema FIEMG.

5. DISPOSIÇÕES GERAIS

5.1. Uso geral da informação

Os terceiros tratarão de forma estritamente confidencial todas as informações levadas a seu conhecimento pelo Sistema FIEMG durante a prestação dos serviços ou em função deles, e somente as utilizarão no âmbito dos serviços ora pactuados.

Obrigam-se, portanto, a manter o sigilo e respeitar a confidencialidade de todos os dados e informações, 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.

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.

5.1.1. 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.

5.1.2. Descarte da informação

Após o término da prestação de serviço, todas as informações obtidas e utilizadas devem ser devolvidas para a FIEMG, devendo enviar um comprovante assinado por seu representante legal certificando tal devolução. Os documentos em papel classificados como confidenciais ou internos, deverão ser fragmentados em pedaços ilegíveis de forma que as informações se tornem irrecuperáveis. Recomenda-se o uso de fragmentadora de papel.

6. DIRETRIZES

6.1. Proteção das informações

Todas as informações produzidas, individualmente ou em conjunto, pelos terceiros a serviço do Sistema FIEMG, originadas ou derivadas de suas atividades de trabalho são

consideradas de nossa propriedade, aplicando-se isso também para qualquer informação provida ou licenciada pela organização.

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

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

6.1.1 Restrição de acesso à informação

O acesso à informação e às funções de sistemas e aplicações são restritos de acordo com o Controle de Acesso. Os requisitos detalhados 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 sensíveis.

6.2. Proteção de Dados Pessoais

Os terceiros deverão conhecer a legislação aplicável à proteção de dados pessoais e à privacidade de seus titulares (a Lei nº 13.709/2018 (LGPD) e *General Data Protection Regulation* (EU GDPR) – (EU) 2016/679) , bem como dispor dos meios necessários e suficientes à efetiva aplicação destes dispositivos legais 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.

6.3. Acesso físico

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

6.4. Uso dos recursos de tecnologia

6.4.1. Rede cabeada, *Wifi* e Internet

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

6.4.2. Fornecimento de recursos ou dispositivos corporativos

Somente será disponibilizado ao terceiro recurso ou dispositivo corporativo, tal como acesso a sistemas, rede cabeada, correio eletrônico, *pendrives*, HD externo, 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 do Sistema FIEMG.

6.4.3. Uso geral de recursos de tecnologia

Quando da utilização dos recursos de tecnologia fornecidos pela 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 da 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 da FIEMG ou de terceiros.

É vedado, 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*) da FIEMG ou de terceiros, ou que possam danificar ou corromper dados, informações, documentos eletrônicos e arquivos.

6.5. Dispositivos móveis

A FIEMG tem a faculdade de autorizar o uso de dispositivos móveis de propriedade de terceiros para a realização de atividades profissionais. Nesse caso, a compatibilidade dos dispositivos móveis e as demais configurações necessárias para uso no ambiente interno da Entidade é de responsabilidade do terceiro.

A 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.

A FIEMG poderá, no entanto, orientar a aquisição ou fornecer aplicativos específicos necessários para o acesso seguro às informações corporativas em alguns ambientes de tecnologia.

6.5.1. Uso de *software*

O uso de *software* não licenciado e/ou pirata é ilegal e expressamente vedado e será considerado como infração grave a esta política, podendo resultar na rescisão dos contratos com os terceiros e na aplicação de penalidades aos mesmos. Caso seja identificado o uso indevido de *software* ou aplicativo pelo terceiro, a 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 pela FIEMG.

6.5.2. Controle de acesso

Os dispositivos móveis de propriedade de terceiros usados nas instalações da FIEMG devem ser protegidos por senha pessoal ou controles que impeçam o acesso não autorizado. Cada terceiro é responsável pela proteção dos dispositivos físicos contendo informações que estão sob sua guarda.

O acesso lógico ao ambiente da rede interna da 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 da 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 da FIEMG.

6.5.3. Proteção contra ameaças digitais

Os dispositivos móveis de propriedade de terceiros usados nas instalações da 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 da FIEMG, deverá avisar imediatamente a Gerência de Segurança da Informação através do e-mail si@fiemg.com.br ou nos ramais do *Help Desk*.

6.5.4. Atualização do dispositivo

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.

6.5.5. Auditoria e conformidade

Fica a critério da FIEMG fiscalizar, a qualquer momento, sem necessidade de aviso prévio, 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.

6.6. Teletrabalho

Caso necessário e após aprovação e autorização prévia por parte da FIEMG, o terceiro deve agir com máxima diligência, a fim de evitar que informações da FIEMG sejam acessíveis por estranhos ou pessoas não autorizadas, devendo observar, no mínimo, o disposto abaixo.

6.6.1. Local de teletrabalho

Acesso remoto a sistemas, infraestrutura de suporte ao ambiente de tecnologia ou informações da FIEMG só devem ser realizados em locais seguros. A realização de trabalho remoto em áreas onde a privacidade não possa ser obtida, tais como aeroportos, salas de reunião, salas de espera, transportes públicos, restaurantes, entre outros, não deve ser realizada.

6.6.2. Autenticação

Todo acesso remoto a sistemas e ambientes de tecnologia que suportam informações corporativas da 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.

6.6.3. Tráfego de informação

Todo o tráfego de informação realizado durante o trabalho remoto deve ser criptografado conforme os padrões de segurança e confidencialidade estabelecidos pela FIEMG.

6.6.4. 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 da FIEMG.

6.6.5. Monitoramento

Os acessos realizados pelos terceiros durante a sessão de teletrabalho são registrados pela FIEMG e podem ser fiscalizados, a qualquer momento, sem necessidade de aviso prévio.

A FIEMG poderá, a qualquer momento, bloquear o acesso do equipamento à rede corporativa, caso sejam detectadas desconformidades com as políticas, normas e procedimentos vigentes.

6.7. Controles de segurança no ambiente do terceiro

O fornecedor que venha a oferecer serviços em nuvem, processar ou armazenar dados da FIEMG em seu ambiente, deve seguir as seguintes diretrizes de segurança da informação:

6.7.1. Controle de acesso

- Possuir documentado um processo de gerenciamento de acessos;
- 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;
- Dar visibilidade aos procedimentos e controles utilizados para prestar os serviços, como descrito no item acima, em especial, para a identificação e a segregação dos dados da FIEMG, por meio de controles físicos ou lógicos.

6.7.2. Gestão de vulnerabilidade

Prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o 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.

6.7.3. 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 pela FIEMG para a execução dos serviços contratados;
- Informar e dar acesso a FIEMG, quando solicitado, sobre os recursos de gestão adequados ao monitoramento dos serviços contratados.

6.7.4. 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;
- Manter a FIEMG permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

6.7.5. Segurança no desenvolvimento de sistemas

- Desenvolver sistemas levando em consideração os padrões de segurança aceitos pelo mercado;

- Descrever os recursos de segurança e os dados acessados pelas aplicações, os quais devem ser avaliados pela área 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;
- 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.

6.7.6. Armazenamento de dados

Informar e dar acesso a FIEMG, quando solicitado, sobre as medidas de segurança para a transmissão e armazenamento dos dados e informações.

6.7.7. Continuidade de negócios

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

6.7.8. Gestão e retenção de dados

Possuir um processo de execução de *backups*, o qual seja realizado periodicamente nos ativos que armazenam informações da FIEMG, de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes.

6.7.9. Subcontratação de serviços

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

6.7.10. Certificações e auditorias independentes

Informar e dar acesso a 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.

6.8. Gestão de incidentes de Segurança de Informação

Incidentes e não-conformidades de Segurança da Informação que sejam de conhecimento do terceiro devem ser imediatamente relatados à Gerência de Segurança da Informação da FIEMG através dos canais de contato disponíveis.

7. DISPOSIÇÕES FINAIS

7.1. Avaliações periódicas

A 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.

7.2. Situações especiais e exceções

As situações especiais e/ou pedidos de exceção a esta política deverão ser avaliados pela Gerência de Segurança da Informação através dos canais de contato disponíveis.

Caso os usuários 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 a 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.

7.3. Casos omissos

Antes de efetuar ações que possam apresentar risco potencial para as informações e/ou sistemas da FIEMG, o usuário deve consultar a Política de Segurança da Informação para prestadores de serviço e 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 Segurança da Informação através dos canais de contato disponíveis.

7.4. Conformidade

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

a) Ao imediato cancelamento do acesso às instalações da 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.

7.5. Documentos de referência

Código de Conduta para terceiros da FIEMG

https://www7.fiemg.com.br/publicacoes-internas/complienceeouvidoria

Política de Privacidade e Proteção de Dados da FIEMG

https://www7.fiemg.com.br/publicacoes-internas/politicaprivacidade

Programa de Integridade

https://www7.fiemg.com.br/publicacoes-internas/integridade

Políticas, normas e manuais de segurança da informação da FIEMG;

ABNT NBR ISO/IEC 27002 – Código de prática para a gestão da segurança da informação.