POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, PROTEÇÃO DE DADOS E SEGURANÇA CIBERNÉTICA

EIG GLOBAL ENERGY (BRASIL) REPRESENTAÇÕES LTDA.

Junho/2025 – Versão 1.0

ÍNDICE

APRESENTAÇÃO

A Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética ("Política") da EIG GLOBAL ENERGY (BRASIL) REPRESENTAÇÕES LTDA. ("EIG" ou "Gestora"), aplica-se a todos os sócios, Colaboradores, prestadores de serviços e sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da EIG, ou que acesse informações a ela pertencentes. Todo e qualquer usuário de recursos computadorizados da nossa instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática da EIG.

Em linha com as principais discussões e preocupações do mercado, a Política tem como base princípios e procedimentos que asseguram a confidencialidade, a integridade e a disponibilidade dos dados e sistemas de informação utilizados pela EIG.

Sem prejuízo de quaisquer disposições desta política, a EIG também observará, conforme aplicável, eventuais políticas de segurança da informação, proteção de dados e segurança cibernética de seu grupo de controle internacional, de modo a estabelecer ainda mais robustez operacional nas atividades da EIG.

OBJETIVOS

Esta Política tem por objetivo contribuir para o aprimoramento da segurança, tanto informacional quanto cibernética da EIG, estabelecendo medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízo para a consecução de suas atividades.

Em atenção aos dispositivos da Resolução CVM n.º 21/2021 e do Código ANBIMA de Regulação e Melhores Práticas para Administração e Gestão de Recursos de Terceiros, assim como à Lei 13.709, de agosto de 2018 (Lei Geral de Proteção de Dados) a EIG procurou identificar os eventos com maior possibilidade de ocorrência, bem como as informações de maior sensibilidade ("Informações Confidenciais"), com o propósito de mitigar os riscos à sua atividade.

Sendo assim, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da EIG, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais, podendo

tais Informações Confidenciais serem divulgadas para colaboradores, diretores, funcionários, membros de comitês, assessores (incluindo jurídicos ou financeiros) da EIG e suas afiliadas.

Qualquer informação sobre a EIG, ou de qualquer natureza relativa às atividades da empresa e a seus sócios e clientes, obtida em decorrência do desempenho das atividades normais do Colaborador, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pelo Diretor de Risco e *Compliance*.

ABRANGÊNCIA

Este procedimento se aplica a EIG, em atendimento aos requisitos do sistema de gestão de Compliance.

A efetividade desta Política depende da conscientização de todos os Colaboradores e do esforço constante para que seja feito bom uso das Informações Confidenciais e dos Ativos disponibilizados pela EIG ao Colaborador.

Esta Política deve ser conhecida e obedecida por todos os Colaboradores que utilizam os recursos de tecnologia disponibilizados pela Gestora, sendo de responsabilidade individual e coletiva o seu cumprimento.

PREMISSAS E DEFINIÇÕES

Diante da possibilidade de vazamento, alteração, destruição e qualquer outra forma de prejuízo em relação às Informações Confidenciais, o que é de extremo valor para a EIG, dado o princípio fundamental de confiança que a instituição trabalha para manter junto aos seus clientes, a EIG utilizou como linha de estruturação de sua Política, o Guia de Cibersegurança, da ANBIMA, datado de junho de 2021.

O referido documento é um dos principais materiais sobre o tema no Mercado Financeiro, incluindo as melhores referências sobre proteção de dados.

Adiante, a EIG abordará os principais mecanismos e procedimentos de prevenção as ameaças ao patrimônio, à imagem e, principalmente, aos seus negócios.

Todas as diretrizes aqui dispostas são de responsabilidade da Área de *Compliance* da EIG, sob a direção do Diretor de Risco e *Compliance* da instituição.

Ademais, para implementação e monitoramento contínuo da presente Política, a EIG conta com o suporte e assessoria da empresa terceirizada de TI, podendo tal assessoria se dar em nível local ou no âmbito de seu grupo controlador internacional.

PROGRAMA DE SEGURANÇA DA EIG PARTNERS

(i) Identificação de Riscos:

Os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação das instituições, permitindo agilidade na construção e disponibilização de serviços, aplicação dos meios de comunicação, entre outros avanços. Por outro lado, o aumento do uso de tais ferramentas potencializa o vazamento de informações e os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integralidade e a disponibilidade dos dados e/ou dos sistemas das instituições.

As ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade, informações ou ativos de cada organização. As consequências para as instituições podem ser significativas em termos operacionais, de risco de imagem, danos financeiros ou perda de vantagem concorrencial, podendo tais danos serem irreparáveis.

Diante desse cenário, os métodos mais comuns de ataques cibernéticos são os seguintes:

- *Malware* – *softwares* desenvolvidos para corromper computadores e redes:
    - *Vírus*: *software* que causa danos a máquina, rede, *software*s e banco de dados;
    - Cavalo de Troia: aparece dentro de outro *software* e cria uma porta para a invasão do computador;
    - *Spyware*: *software* malicioso para coletar e monitorar o uso de informações; e
    - *Ransomware*: *software* malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.
- Engenharia Social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:
    - *Pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;

    - *Phishing*: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
    - *Vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
    - *Smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;
    - Acesso pessoal; pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.
- Ataques de *DDoS* (*distributed denial of services*) e *botnets* - ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos *botnets*, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar *spam* ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.
- Invasões (*advanced persistent threats*) - ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ainda, além de ataques cibernéticos, a EIG pode estar sujeita ao mau funcionamento dos sistemas utilizados e a atos ou omissões de seus Colaboradores, que podem acarretar no perdimento e/ou adulteração de dados e Informações Confidenciais.

Para a identificação e avaliação de riscos, são realizadas as seguintes ações:

a) Identificação dos ativos relevantes da EIG (sejam equipamentos, sistemas processos ou dados) usados para seu correto funcionamento;
b) Avaliação das vulnerabilidades dos ativos, identificando-se possíveis ameaças e graus de exposição;
c) Mensuração de impacto potencial e probabilidade de ocorrência dos riscos identificados, considerando aspectos financeiros, operacionais e reputacionais.

(ii) <u>Ações de Prevenção e Proteção</u>

Para que se possam prevenir eventuais ataques cibernéticos e vazamento de informações, primeiro deve-se definir quais informações são as de maior sensibilidade para a EIG, assim como aquelas que teriam o maior impacto financeiro, operacional e reputacional para EIG, em caso de incidente de segurança.

Deste modo, a EIG segrega as informações geradas pela instituição, aperfeiçoando a implementação de processos e o devido manuseio, armazenamento, transporte e descarte destas informações.

Assim, classificam-se as informações digitais da instituição em 3 (três) classes diferentes, quais sejam:

a) *Green Flag:*

- Quaisquer informações e/ou dados que a EIG teve acesso ou conhecimento por ser de domínio público ("Informação Pública");
- Quaisquer informações e/ou dados que não estejam sujeitas a compromissos ou acordos de confidencialidade; ou
- Quaisquer informações e/ou dados que tenham a obrigatoriedade de divulgação por lei ou autoridade competente.

b) *Yellow Flag:*

- Quaisquer informações que venham a ter a obrigatoriedade de divulgação por lei ou autoridade competente, mas o termo legal ainda não foi iniciado ou findado (Ex. Data de Divulgação);

c) *Red Flag:*

- Todas as Informações Confidenciais, a saber:
- know-*how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras, estatísticas, logísticas ou relacionadas às estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e/ou dos fundos geridos pela EIG;
- operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela EIG; e
- estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da EIG e/ou de seus sócios e clientes.

A partir da definição acima, a EIG se empenhará para manter controles, conforme o nível de criticidade das informações e dados, sendo certo de que a prioridade será escalonada na seguinte ordem de relevância: *Red Flag, Yellow Flag* e *Green Flag*.

A partir desse ponto, passamos a mencionar os procedimentos de prevenção e proteção adotados pela EIG:

Estrutura de TI

I. Uso dos Recursos de TI

Todos os recursos computacionais e de sistemas disponibilizados para os Colaboradores são de propriedade e/ou com licenças da EIG.

II. Disponibilização e uso

Todos os computadores disponibilizados para os Colaboradores da EIG têm por objetivo o desempenho das atividades profissionais na EIG.

Conforme anteriormente citado, todo o processo de criação e exclusão de usuário, instalação de *software*s e aplicativos, permissão de acesso, entre outras funcionalidades informáticas, são realizados pela área responsável, com supervisão do Diretor de Risco e *Compliance*.

A disponibilização e uso dos computadores da EIG respeitam as seguintes regras:

- A cada novo Colaborador, a área de tecnologia, em consulta com o Diretor de Risco e *Compliance*, autorizará, a criação de novo usuário e a disponibilização técnica de recursos;
- Todos os equipamentos, *software*s e permissões acessos devem ser testados, homologados e autorizados pela área responsável, mediante supervisão do Diretor de Risco e *Compliance*;
- O Diretor de Risco e *Compliance* autorizará, mediante solicitação, a retirada ou substituição do computador disponibilizado para o usuário;
- Cada computador tem o seu usuário gestor, que é responsável por esse equipamento. O controle das máquinas é de responsabilidade da área responsável;
- A identificação do usuário é feita através do *login* e senha, que através do registro de *logs* utilizado pela EIG é sua assinatura eletrônica no servidor da EIG;
- Será apenas permitida senhas com no mínimo 08 (oito) caracteres alfanuméricos, maiúsculos e minúsculos. A eventual reutilização de senhas obedecerá ao ciclo mínimo de 05 (cinco) vezes;
- Não será permitida a utilização da mesma senha para projetos e serviços diferentes realizados pela EIG, não devendo ser criada uma senha única padrão para todos os serviços e áreas em que um mesmo Colaborador atue;
- É permitida apenas 3 tentativas máximas de autenticação de senha, sendo todas malsucedidas, será bloqueado o acesso, o qual apenas poderá ser reestabelecido

através de solicitação para a área de tecnologia e/ou ao Diretor de Risco e *Compliance* que acionará a primeira.

- A senha possui validade de 180 (cento e oitenta) dias e sua troca será solicitada automaticamente quando da expiração da mesma.
- Todos os eventos de *login* e alteração de senhas são auditáveis e rastreáveis, podendo ser solicitados pelo Diretor de Risco e *Compliance* à área responsável.

III. Softwares

A implantação e configuração de *software*s da EIG s respeitam as seguintes regras:

- Todos os *software*s, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela área responsável, mediante supervisão do Diretor de Risco e *Compliance;*
- É desabilitado aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada da área de tecnologia, em consulta com o Diretor de Risco e *Compliance*;
- É desabilitado ao usuário implantar ou alterar componentes físicos em seus computadores;
- Somente é permitido o uso de equipamentos homologados e devidamente contratados pela EIG;
-
- A conexão de dispositivos móveis de armazenamento (e.g. *USB Drive*) somente poderá ser realizada mediante autorização prévia e expressa da área de tecnologia, em consulta com o Diretor de Risco e *Compliance*.

IV. Registros

A EIG mantém por 5 anos todos os *logs* de sistemas, e verifica regularmente, quaisquer desvios de padrão de todos os computadores, arquivos em rede, sejam *software*s, *hardwares* ou acessos que não sejam autorizados.

Nesse sentido, através dos logs realizados pela EIG, a Gestora consegue manter a integridade, autenticidade e auditabilidade das informações e sistemas, conforme Resolução CVM n.º 21/2021.

V. Responsabilidades do usuário

O Colaborador é o custodiante dos recursos disponibilizados a ele, devendo este cuidar adequadamente do equipamento.

O Colaborador também deve garantir a sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pela EIG.

Ainda, o Colaborador deve adotar um comportamento seguro condizente com a Política, devendo:

- Não compartilhar nem divulgar sua senha a terceiros;
- Não transportar Informações Confidenciais da EIG em qualquer meio (CD, DVD, *pendrive*, papel, etc.) sem as devidas autorizações e proteções;
- Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais, etc.);
- Não abrir mensagens de origem desconhecida, ou links suspeitos mesmo que advindos de origem conhecida;
- Armazenar e proteger adequadamente documentos impressos e arquivos eletrônicos que contêm Informações Confidenciais; e
- Seguir corretamente a política para uso de internet e correio eletrônico estabelecida pela EIG.

VI. Outras Proteções aos Computadores

- Proteção de tela no computador e/ou proteção de ausência (após um tempo de inatividade, o computador bloqueia o sistema, exigindo senha para ser usado novamente);
- "Log-*off*" automático por inatividade durante o período de 24 horas;
- Bloqueio do acesso as portas *USB* dos computadores para proteção contra vírus e cópia indevida dos dados contidos nos servidores;
- Bloqueio do acesso a sites de armazenamento de dados em Nuvem (*Cloud*);
- Bloqueio de sistemas de gerenciamento de computador à distância.

VII. Regras e responsabilidades do uso da Internet

O Colaborador é responsável por todo acesso realizado com a sua autenticação.

Quando o usuário se comunicar através de recursos de tecnologia da EIG, este deve sempre resguardar a imagem da EIG, evitando entrar em sites de fontes não seguras, assim como de abrir e-mails pessoais, ou, de fontes não conhecidas, salvo quando comunicado e devidamente autorizado pelo Diretor de Risco e *Compliance*.

O usuário é proibido de acessar endereços de internet (sites) que:

- Possam violar direitos de autor, marcas, licenças de programas (*software*s) ou patentes existentes;
- Possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia;
- Contenham informações que não colaborem para o alcance dos objetivos da EIG;
- Defendam atividades ilegais, menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física;
- Possuam origem suspeita ou que não se atenham aos padrões de segurança adequados, assim como possuírem links suspeitos.

O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes e que o uso do material foi autorizado, no mínimo, pelo gestor da sua área.

O uso de serviços de mensagem instantânea para fins profissionais deve seguir as políticas estabelecidas pelo grupo controlador do EIG.

Também se faz expressamente proibido o uso de serviços de rádio, streaming, download de vídeos, filmes e músicas, através dos computadores da EIG.

VIII. Bloqueio de endereços de Internet

Periodicamente, a Área de *Compliance* irá revisar e bloquear o acesso para os endereços da Internet que não estejam alinhados com esta Política e com o Código de Ética da EIG.

IX. Uso de correio eletrônico particular

É proibido a utilização profissional de correio eletrônico particular.

A EIG disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais. (ex.: usuario@eigpartners.com)

O endereço eletrônico disponibilizado para o usuário é individual, intransferível e pertence à EIG.

O endereço eletrônico cedido para o usuário deve ser o mesmo durante todo o seu período de vínculo com a EIG.

Se houver necessidade de troca de endereço, a alteração será realizada pela área responsável, mediante autorização e supervisão do Diretor de Risco e *Compliance*.

X. Endereço eletrônico de programas ou de comunicação corporativa

É permitida a existência de endereços de correio eletrônico para o envio de mensagens tipo Comunicação Interna da EIG, porém, é obrigatória a identificação do usuário que encaminhou a mensagem.

O endereço de correio eletrônico disponibilizado para os Colaboradores e as mensagens associadas a este correio eletrônico são de propriedade da EIG.

XI. Acesso à distância ao e-mail

O usuário pode acessar o seu correio eletrônico cedido pela EIG mesmo quando estiver fora do ambiente da empresa, através do serviço de correio eletrônico via Internet.

O Colaborador deve ter o mesmo zelo com a utilização do correio eletrônico à distância tal qual estivesse no ambiente físico da EIG.

XII. Responsabilidades e forma de uso de Correio Eletrônico

O Colaborador que utiliza um endereço de correio eletrônico é responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail, podendo enviar mensagens necessárias para o seu desempenho profissional na EIG.

É proibido criar, copiar ou encaminhar mensagens ou imagens que:

- Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
- Façam parte de correntes de mensagens, independentemente de serem legais ou ilegais;
- Repassem propagandas ou mensagens de alerta sobre qualquer assunto. Havendo situações em que o usuário ache benéfico divulgar o assunto para a EIG, a sugestão deve ser encaminhada para a Área de Recursos Humanos, que definirá a sua publicação ou não;
- Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física;

- Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional;
- Sejam suscetíveis de causar qualquer tipo de prejuízo a terceiros;
- Defendam ou possibilitem a realização de atividades ilegais;
- Sejam ou sugiram a formação ou divulgação de correntes de mensagens;
- Possam prejudicar a imagem da EIG; e
- Sejam incoerentes com o Código de Ética Corporativa da EIG.

É proibido reproduzir qualquer material recebido pelo correio eletrônico ou outro meio, que possa infringir direitos de autor, marca, licença de uso de programas ou patentes existentes, sem que haja autorização expressa do autor do trabalho e da organização.

O Colaborador deve estar ciente que uma mensagem de correio eletrônico da EIG é um documento formal e, portanto, possui as mesmas responsabilidades de um documento convencional em papel timbrado da entidade.

Exceto quando especificamente autorizado para tal, é proibido emitir opinião pessoal, colocando-a em nome da EIG.

Deve observar se o endereço do destinatário corresponde realmente ao destinatário desejado.

O Colaborador deve ser diligente em relação:

- Aos usuários que receberão a mensagem (Destinatário/ To, Copiado/Cc e Copiado Oculto/Bcc);
- Ao nível de sigilo da informação contida na mensagem;
- Aos anexos da mensagem, enviando os arquivos apenas quando for imprescindível e garantindo a confidencialidade dos mesmos;
- Ao uso da opção encaminhar (*Forward*), verificando se é necessária a manutenção das diversas mensagens anteriores que estão encadeadas.

O Colaborador deve deixar mensagem de ausência quando for passar um período maior do que 24 (vinte e quatro) horas sem acessar seu correio eletrônico. Essa mensagem deve indicar o período de ausência e o endereço do substituto para quem deve ser enviada a mensagem.

XIII. Cópias de segurança do Correio Eletrônico

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria a cópia de segurança das mensagens de correio eletrônico é feita de forma centralizada no ambiente dos equipamentos servidores corporativos, sob a responsabilidade da área responsável, mediante supervisão do Diretor de Risco e *Compliance*.

XIV. Armazenamento em Nuvem (*Cloud*)

A EIG poderá realizar o armazenamento das Informações Confidenciais e quaisquer outros dados na Nuvem (*Cloud*).

De forma a possuir um ambiente seguro de nuvem, considerando aplicações WEB, se prezará pela confiabilidade, disponibilidade e integridade do armazenamento da mesma.

XV. Contratação de Terceiros para Serviços de Armazenamento na Nuvem

Fornecedores, prestadores de serviços e parceiros ("Terceiros") podem representar uma fonte significativa de riscos para a EIG em relação à Cibersegurança. Neste sentido, é necessário adotar certos procedimentos que devem ser realizados previamente a contratação de Terceiros para serviços de Armazenamento na Nuvem, conforme o nível de diligência previsto nas políticas aplicáveis dos controladores do EIG.

SEGREGAÇÃO DE ATIVIDADES

A segregação das atividades de administração de carteira de valores mobiliários tem por objetivo evitar que ocorram diversos problemas de conflito de interesses e uso indevido de informações privilegiadas, bem como criar os procedimentos e controle que permitirão uma maior qualidade do serviço.

A EIG reconhece que a segregação das atividades é um requisito essencial para o efetivo cumprimento às suas estratégias de administração de recursos de terceiros, uma vez que cumpre um papel importantíssimo na defesa dos interesses de seus clientes.

Logo, a EIG segrega suas diversas áreas a partir dos procedimentos operacionais por ela adotados e cada funcionário da EIG possui seu próprio microcomputador e telefone de uso exclusivo, de modo a evitar o compartilhamento do mesmo equipamento e/ou

a visualização de informações de outro funcionário, mantendo ainda outros procedimentos que auxiliar o cumprimento.

Ainda nesse sentido acesso a informações relativas à administração de recursos de terceiros é restrito aos empregados que necessitem desta informação para exercerem suas funções na exata medida que isto for necessário, a critério do Diretor Responsável ("Pessoas Autorizadas"). Isto também se refletirá nos sistemas de gerenciamento da informação, nos quais cada usuário terá uma amplitude de acesso limitada e que permitirá o controle do que é acessado, por quem e quando é acessado.

Ademais, cada colaborador possui um código de usuário e e-mail. Ainda, a rede de computadores da EIG permite a criação de usuários com níveis de permissão diferentes, por meio de uma segregação lógica nos servidores da empresa que garantem áreas de armazenamento de dados distintas no servidor com controle de acesso por usuário. Além disso, a rede de computadores mantém um registro de acesso de cada arquivo, que permite identificar as pessoas que acessam cada dado ou informação. Cada colaborador tem à disposição uma pasta própria de acesso exclusivo para digitalizar os seus arquivos, garantindo acesso exclusivo do usuário aos documentos de sua responsabilidade.

Sendo assim, a EIG acredita que as medidas acima relacionadas são eficazes para cumprir os requisitos mínimos de segregação de atividades aplicados a sua realidade, estando sempre em busca de servir adequadamente seus clientes e cumprir com suas obrigações fiduciárias.

DESLIGAMENTO DE COLABORADORES

No caso desligamento de Colaboradores, a Área de *Compliance* irá solicitar ao TI terceirizado o imediato desligamento de todos os acessos deste Colaborador, dentre os quais acesso ao banco de dados e ao e-mail corporativo.

Da mesma maneira, caso o Colaborador seja transferido de área, este deverá ter seus acessos adequados à sua nova função, de forma a não dispor de acesso às informações incompatíveis com as atividades executadas.

MONITORAMENTO E TESTES PERIÓDICOS

O monitoramento dos controles existentes e estabelecidos nessa Política serão realizados pelas áreas de tecnologia, incluindo do controlador do EIG, e conforme aplicável com sob supervisão do Diretor de Risco e *Compliance*. O referido monitoramento acontecerá de forma contínua, sem periodicidade.

Os Testes de Contingência serão realizados anualmente conforme as políticas do grupo de controle internacional do EIG, e de modo a permitir que a EIG esteja preparada para a continuação de suas atividades, assim como a mitigar eventuais riscos operacionais ou reputacionais. Outras informações acerca dos Testes de Contingência estão no Plano de Continuidade de Negócios da EIG.

PLANO DE RESPOSTA

Conforme as melhores práticas de mercado, a EIG desenvolveu um Plano de Resposta para indícios, suspeita fundamentada, vazamento de Informações Confidenciais ou outra falha de segurança.

Na hipótese de verificação de uma das hipóteses acima, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas, devendo cada área responsável agir conforme o disposto na presente Política.

A primeira providência é a consulta imediata com os times de tecnologia e segurança cibernética do grupo de controle internacional do EIG, que adotará as providências cabíveis. As providencias secundárias em nível local podem consistir em:

Empresa de TI Terceirizada (Sob Supervisão do *Compliance*):

a) Verificação e Auditoria dos *Logs*;
b) Criação de laudo pericial contendo as informações que foram potencialmente vazadas;
c) Execução de aplicativos externamente ou em sistemas afetados para eliminar aplicativos indesejados;
d) Desinstalação de *software*;
e) Execução de varreduras *offline* para descobrir quaisquer ameaças adicionais;
f) Formatação e reconstrução do sistema operacional;
g) Substituição física de dispositivos de armazenamento
h) Reconstrução de sistemas e redes;
i) Restauração de dados provenientes do backup realizado diariamente;

j) Entre outros.

Compliance ou Jurídico Contratado:

a) Criação de relatório baseado no laudo pericial elaborado pela Empresa de TI Terceirizada, de forma a constar eventuais consequências reputacionais e jurídicas derivadas dos danos ocasionados pelo incidente de segurança;
b) Em caso de confirmação do incidente de segurança e eventual vazamento de informações confidenciais, elaborar notificação aos clientes afetados informando o ocorrido.

BackOffice:

a) Análise de dados perdidos e suas influências frente ao planejamento contábil e aos ativos da Companhia;
b) Realizar planejamento de contenção de risco de liquidez frente a possibilidade de resgate de investimentos da EIG resultantes do incidente de segurança.

Em caso de necessidade, poderá ser contratada empresa especializada no combate ao evento identificado, assim como nas respostas ao eventual dano.

Todo e qualquer incidente ocorrido, assim como os resultados do Plano de Resposta, deverão ser devidamente classificados por nível de severidade, arquivados e documentados pela Área de *Compliance*, bem como ser formalizado no Relatório de Controles Internos da EIG.

A EIG Partners deverá realizar, em caso de incidente que afetem os dados pessoais que realize tratamento, a comunicação tempestiva às partes afetadas, bem como à Autoridade Nacional de Proteção de Dados ("ANPD")

Caso o evento tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade, nos termos do Código de Ética da EIG.

PROTEÇÃO DE DADOS PESSOAIS

Escopo e Abrangência:

A EIG está comprometida em preservar a privacidade de dados pessoais e de dados sensíveis que forem coletados ou aos quais tiver acesso em função do uso do site ou por conta do desempenho de suas atividades, e com o cumprimento das leis e regulamentos em vigor.

Por conta disso, estabeleceu, as diretrizes, princípios e regras previstas nesta Política, as quais servirão de guia para a coleta, registro, processamento, armazenamento, uso, compartilhamento e eliminação de dados pessoais, fornecendo o arcabouço para o correto tratamento e proteção dos dados pessoais em seu poder.

Essas diretrizes, princípios e regras se aplicam a todos os Colaboradores da EIG, e englobam os dados pessoais que se encontrem armazenados em qualquer meio, e abrangem toda e qualquer forma de tratamento que possa ser empregada e esteja disponível para a EIG.

Importante observar que o escopo da proteção de dados pessoais no âmbito da EIG está, em grande parte, limitado aos dados pessoais de seus Colaboradores e de pessoas físicas e jurídicas com as quais tiver estabelecido relações jurídicas, com especial menção ao cumprimento da regulação aplicável à gestão de recursos de terceiros. Também estão abrangidos por esta proteção os dados de candidatos às vagas na Gestora, de fornecedores e outros com os quais a EIG manteve contato para atender alguma demanda relevante e específica.

Vale ressaltar que todo o tratamento de dados pessoais feito pela EIG Partners está pautado nos requisitos do artigo 7º da Lei 13.709/2018 (“LGPD”), assim como nas premissas do artigo 11 da mesma Lei, quando aplicável.

Princípios Norteadores:

A EIG Partners compromete-se a obter dados pessoais de maneira justa e legal, e suas ações serão norteadas no princípio da boa-fé e nos princípios abaixo, os quais estão elencados no art. 6º da LGPD:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X – responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Direitos:

Em respeito aos direitos fundamentais de liberdade, de intimidade e de privacidade, e, ainda, ao disposto no art. 18 da LGPD, o titular dos dados pessoais tem direito de solicitar à EIG Partners, em relação aos seus dados, a qualquer momento e mediante requerimento expresso o que se segue.

a) confirmação de existência de tratamento;

b) acesso aos dados;

c) correção de dados incompletos, inexatos ou desatualizado;

d) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei 13.709/2018;

e) portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

f) eliminação dos dados pessoais tratados com o consentimento do titular, exceto em determinadas situações e respeitados os limites técnicos das atividades, conforme determinado na Lei;

g) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

h) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e

i) revogação do consentimento, nos termos da Lei.

Período de Armazenamento dos Dados Pessoais:

Os dados pessoais serão armazenados pela EIG durante tempo necessário para o atingimento dos objetivos para os quais foram coletados. De todo modo, este período poderá ser ampliado para o cumprimento de obrigação legal, regulatória ou contratual, pelo que, nestas hipóteses o prazo mínimo de armazenamento será de 5 (cinco) anos.

Cooperação com Autoridades:

A divulgação de dados pessoais para o cumprimento de lei, determinação judicial, regulatória ou de órgão competente ao qual a EIG estiver sujeita somente ocorrerá nos estritos termos e nos limites requeridos para o cumprimento da obrigação, sendo que os titulares dos dados, na medida do possível e desde que não configure infração, inadimplemento ou cause prejuízo à EIG, serão notificados sobre tal divulgação, para que tomem as medidas apropriadas.

Adicionalmente, a EIG cooperará com a ANPD em qualquer problema em relação à proteção de dados e dentro dos limites previstos na LGPD e nas demais

regulamentações sobre a matéria, porém sem renunciar a quaisquer defesas e/ou recursos disponíveis.

Governança:

As matérias relacionadas aos dados pessoais, dados sigilosos e ao tratamento destes, serão apresentadas para deliberação no Comitê de Gestão de Riscos e de Compliance.

Obrigação de Reporte:

Os Colaboradores estão obrigados a comunicar imediatamente ao Diretor de Risco e *Compliance* sobre toda e qualquer suspeita ou indício de evento que possa ter comprometido os dados pessoais de posse da EIG para a devida apuração. Caso necessário, o Diretor de Risco e *Compliance* notificará, em prazo compatível com a severidade do evento, a ANPD, bem como todos os que porventura possam ter sido afetados pelo referido evento.

Registro de Eventos:

Os eventos reportados que tenham sido apurados e tiverem resultado no comprometimento de dados pessoais serão registrados no Relatório de Controles Internos e no Relatório de Impacto à Proteção de Dados Pessoais, inclusive de dados sensíveis, nos termos do artigo 38 da LGPD.

Treinamento:

A EIG treinará periodicamente seus Colaboradores sobre a proteção de dados pessoais e de dados sigilosos de acordo com a sua Política de Treinamento e Reciclagem de Colaboradores.

VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada periodicamente, pelo menos 01 (uma) vez ao ano, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

O objetivo principal do processo de revisão dessa Política é manter sempre atualiza a metodologia de avaliação de risco, as implementações de proteção e prevenção, os monitoramentos e testes e os planos de resposta.

CONTROLE DE VERSÕES	DATA	MODIFICADO POR	DESCRIÇÃO DA MUDANÇA
1	Junho/2025	RRZ Consultoria	Versão inicial

ANEXO I - TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Nesta data, eu, _____, inscrito no CPF/ME sob o nº _____ , declaro que li e estou plenamente de acordo com as disposições da Política de Segurança da Informações e Segurança Cibernética da EIG GLOBAL ENERGY (BRASIL) REPRESENTAÇÕES LTDA. Comprometo-me a cumprir com os termos dispostos na mesma, preservando a confidencialidade das informações as quais terei acesso.

[CIDADE], [DIA] de [MÊS] de 202[●].

_____

[Assinatura]