Política de Segurança da Informação e Cibernética

RIZA | SEC

RIZA | SEC

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

INTRODUÇÃO

A Política de Segurança da Informação e Segurança Cibernética ("Política") da Riza SEC, aplica-se a todos os sócios, diretores, colaboradores e estagiários, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento ou a quem acesse informações a ele 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.
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 Riza SEC.

OBJETIVO

Esta Política tem por objetivo contribuir para o aprimoramento da segurança, tanto informacional quanto cibernética da Riza SEC, estabelecendo medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízo para suas atividades.
Sendo assim, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Riza SEC, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.
Qualquer informação sobrea Riza SEC, ou de qualquer natureza relativa às atividades da empresa e a seus sócios e clientes, obtida em decorrência do fornecida ao público, mídia ou a demais órgãos caso autorizado pela Diretora de Compliance.

ABRANGÊNCIA

Aplica-se a todos os colaboradores, estagiários, administradores, diretores estatutários, membros de comitês, parceiros, prestadores de serviço, terceiros contratados e quaisquer pessoas físicas ou jurídicas que atuem direta ou indiretamente em nome da Riza Securitizadora.

VIGÊNCIA

Esta Política tem a vigência de dois anos a partir de sua publicação, devendo ser revisada e atualizada em caso de alterações de normativos ou mudança significativa do sistema de controles internos da Instituição.

DIRETRIZES

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 Riza SEC, dado o princípio fundamental de confiança mantido junto aos seus clientes.
Todas as diretrizes aqui dispostas são de responsabilidade da Área de Compliance da Riza SEC, sob a direção da Diretora de Compliance.
Ademais, para implementação e monitoramento contínuo da presente Política, a Riza SEC conta com o suporte e assessoria de TI interno.

PROGRAMA DE SEGURANÇA DA RIZA:

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 à máquina, rede, softwares 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;
- 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 muitos 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 Riza SEC pode estar sujeita a mal funcionalidades dos sistemas utilizados e a atos ou omissões de seus Colaboradores, que podem acarretar o perda e/ou adulteração de dados e Informações Confidenciais.

Propriedade dos Recursos de TI:

Todos os recursos computacionais e de sistemas disponibilizados para os Colaboradores são de propriedade da Riza SEC. Não é permitida a utilização de notebooks, tablets ou outros hardwares para operações, salvo expressa permissão da Diretora de Compliance.

Disponibilização e uso:

Todos os computadores disponibilizados para os Colaboradores da Riza SEC têm por objetivo o desempenho das atividades profissionais, não devendo ser utilizado para quaisquer outros fins.
Conforme anteriormente citado, todo o processo de criação e exclusão de usuário, instalação de softwares e aplicativos, permissão de acesso, entre outras funcionalidades informáticas, são realizados pelo TI.
A disponibilização e uso dos computadores da Riza SEC respeitam as seguintes regras:

· A cada novo Colaborador, mediante solicitação ao TI, a criação de novo usuário e a disponibilização técnica de recursos será realizada;
· Todos os equipamentos, softwares, permissões e acessos devem ser testados, homologados e autorizados pelo TI, mediante supervisão da Diretora de Compliance.
· a Diretora de 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 do TI, mediante supervisão da Diretora de Compliance.
· A identificação do usuário é feita através do login e senha, que através do registro de logs utilizado pela Riza SEC é sua assinatura eletrônica no servidor.
· Não será permitida a utilização da mesma senha para projetos e serviços diferentes realizados pela Riza SEC não devendo ser criada uma senha única padrão para todos os serviços e áreas em que um mesmo Colaborador atue.
· Todos os eventos de login e alteração de senhas são auditáveis e rastreáveis, podendo ser solicitados pela Diretora de Compliance.

Softwares:

A implantação e configuração de softwares da Riza SEC respeitam as seguintes regras:
· Todos os softwares, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pelo TI, mediante supervisão da

Diretora de Compliance.

· É desabilitado aos usuários implantar novos programas ou alterar configurações sem a permissão do TI.

· É desabilitado ao usuário implantar ou alterar componentes físicos em seus computadores.

· Somente é permitido o uso de equipamentos homologados e devidamente contratados.

· A utilização de equipamentos pessoais por terceiros nas instalações da Riza SEC e a conexão destes na rede interna à Internet requer autorização prévia e expressa. Os Colaboradores estão autorizados a conectar seus telefones celulares e computadores pessoais diretamente à rede interna e à Internet, desde que utilizem suas credenciais de acesso.

· A conexão de dispositivos móveis de armazenamento (e.g. USB Drive) somente poderá ser realizada mediante autorização prévia e expressa da Diretora de Compliance.

Registros:

A Riza SEC mantém por 05 (cinco) anos todos os logs de sistemas, e verifica regularmente, quaisquer desvios de padrão de todos os computadores, arquivos em rede, sejam softwares, hardwares ou acessos que não sejam autorizados.

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 Riza SEC.

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 Riza SEC 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 Riza SEC.

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 Service) não aprovados.
· Bloqueio de sistemas de gerenciamento de computador à distância.

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 Riza SEC, este deve sempre resguardar a imagem da companhia, 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 pela Diretora de Compliance.

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

· Possam violar direitos de autor, marcas, licenças de programas (softwares) ou patentes existentes.
· Conteúdo que envolva pornografia, práticas sexuais explícitas, exploração infantil ou qualquer material relacionado a crimes de pedofilia.
· Contenham informações que não colaborem para o alcance dos objetivos da Riza SEC.
· 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.

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

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 e Conduta.

Uso de correio eletrônico particular:

É proibido a utilização profissional de correio eletrônico particular.
A Riza SEC disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais. (ex.: usuario@rizasec.com)
O endereço eletrônico disponibilizado para o usuário é individual, intransferível e pertence à companhia.
O endereço eletrônico cedido para o usuário deve ser o mesmo durante todo o seu período de vínculo com a Riza SEC. Se houver necessidade de troca de endereço, a alteração será realizada pelo TI.
Endereço eletrônico de programas ou de comunicação corporativa:
É permitido que um programa aplicativo ou um programa de sistema possua um endereço de correio eletrônico. Nesse caso, é obrigatória a existência de um usuário da Área de Compliance responsável por acompanhar as mensagens emitidas e recebidas por esse endereço.
É permitida a existência de endereços de correio eletrônico para o envio de mensagens tipo Comunicação Interna da Riza SEC, 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 Riza SEC.

Acesso à distância ao e-mail:

O usuário pode acessar o seu correio eletrônico cedido pela Riza SEC 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 Riza SEC.

RIZA | SEC

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.

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 Companhia, 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 susceptíveis 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 Riza SEC; e
· Sejam incoerentes com o Código de Ética e Conduta.

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 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 Riza SEC.
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; e
· 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.

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 do TI.

Armazenamento em Nuvem (Cloud):

A Riza SEC realiza o armazenamento das Informações Confidenciais e quaisquer outros dados na Nuvem (Cloud Service).
De forma a possuir um ambiente seguro de nuvem, considerando aplicações WEB, se prezará pela confiabilidade, disponibilidade e integridade do armazenamento da mesma.
Fornecedores, prestadores de serviços e parceiros (“Terceiros”) podem representar uma fonte significativa de riscos para a Riza SEC em relação à Cibersegurança. Neste sentido, necessário adotar certos procedimentos que devem ser realizados previamente a contratação de Terceiros para serviços de Armazenamento em Nuvem. Necessário iniciar um devido processo de Due Diligence do Terceiro antes da contratação, devendo-se constatar se a organização segue políticas, programas e procedimentos formais relativos à segurança da informação e cibersegurança.

Com isto em mente, a empresa objeto de contratação deverá enviar a Riza SEC:

- Documentos que atestem a existência dos respectivos procedimentos de Cibersegurança;

- Último relatório de teste/auditoria periódica; e
- As certificações que possam comprovar a devida capacidade técnica do prestador de serviço.

Uma vez recebidos os respectivos documentos, a Área de Tecnologia analisará o Terceiro, podendo negar de imediato a contratação deste ou exigir remediações para que este se encaixe nos moldes de segurança a serem aplicados.
Somente após a aprovação pela Área de Tecnologia, o Terceiro poderá ser contratado para prestar serviços de Armazenamento na Nuvem.
Em caso de qualquer incidente constatado pelo Terceiro, este deverá de imediato enviar uma notificação relatando o ocorrido, à Riza SEC, a qual, dependendo da situação, poderá reavaliar e inclusive rescindir de imediato o contrato do Terceiro.
Outros serviços com utilização da tecnologia em Nuvem também devem ser considerados para fins das regras aqui presentes, sendo necessário aplicar os mesmos procedimentos de Due Dilligence aos provedores destes serviços, tal como, porém, não exclusivamente:

- Software as a Service (SaaS) – utilização do software do provedor por meio de subscrição, eliminando a necessidade de instalação e execução nos computadores;
- Platform as a Service (PaaS) – desenvolvimento, teste, uso e controle sobre softwares próprios; e
- Infrastructure as a Service (IaaS) – utilização e controles sobre softwares próprios e de terceiros, sistemas operacionais, servidores, unidades de armazenamento e rede – contratação de servidores virtuais

MONITORAMENTO E TESTES DE CONTINGÊNCIA:

O monitoramento dos controles existentes e estabelecidos nessa Política serão realizados e executados pelo TI, sob supervisão da Diretora de Compliance. O referido monitoramento acontecerá de forma contínua, sem periodicidade.
Os Testes de Contingência serão realizados anualmente, de modo a permitir que a Riza SEC 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.

Ademais, serão realizados Testes Periódicos de Segurança, com especial enfoque em segregação lógica, testes de penetração, resposta a eventos de vazamento de dados, rastreabilidade dos logs de acessos às informações sensíveis, tratamento de dados,

dentre outros, sempre objetivando a preservação dos dados mantidos pela Riza SEC, em especial os confidenciais.
Referidos testes serão realizados, com periodicidade mínima semestral, pela empresa de TI terceirizada e o resultado será consolidado no relatório anual de controles internos.

PLANO DE RESPOSTA:

Conforme as melhores práticas de mercado, a Riza SEC 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.

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 Riza SEC.
A Riza SEC 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 e Conduta.

PROTEÇÃO DE DADOS:

Escopo e Abrangência:

A Riza SEC 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 Riza SEC, 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.
Importante observar que o escopo da proteção de dados pessoais no âmbito da Riza SEC está, em grande parte, limitado aos dados pessoais de seus Colaboradores e de pessoas físicas e jurídicas com as quais tiver estabelecido relações jurídicas.

Também estão abrangidos por esta proteção os dados de candidatos às vagas na companhia, de fornecedores e outros com os quais mantiveram contato para atender alguma demanda relevante e específica.
Vale ressaltar que todo o tratamento de dados pessoais feita pela Riza SEC 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 Riza SEC 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 Riza SEC, 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.

A Riza SEC disponibiliza canal de comunicação, através do endereço dpo@rizasec.com, por meio do qual o seu Encarregado pelo Tratamento de Dados Pessoais, receberá quaisquer requisições, solicitações, comunicações e/ou manifestações dos titulares de dados pessoais para exercício dos direitos estipulados na Lei Geral de Proteção de Dados em consonância a sua Política de Privacidade.

O Encarregado pelo Tratamento de Dados Pessoais, também conhecido como Data Protection Officer (DPO), é o responsável por auxiliar os controladores de dados pessoais em relação ao cumprimento de suas obrigações legais referentes à privacidade.

Dessa forma, o DPO atua como uma ponte entre a Riza SEC, os titulares dos dados (pessoas físicas) e a ANPD.

Período de Armazenamento dos Dados Pessoais:

Os dados pessoais serão armazenados pela Riza SEC durante tempo necessário para o atingimento dos objetivos ou do cumprimento regulatório mínimo de acordo com os normativos aplicáveis a Instituição 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 à Riza SEC 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 organização, serão notificados sobre tal divulgação, para que tomem as medidas apropriadas.

Adicionalmente, a Riza SEC 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 aos tratamentos destes, serão apresentados pelo Encarregado pelo Tratamento de Dados Pessoais para deliberação no Comitê de Riscos e Compliance.

Obrigação de Reporte:

Os Colaboradores estão obrigados a comunicar imediatamente ao Encarregado pelo Tratamento de Dados Pessoais sobre toda e qualquer suspeita ou indício de evento que possa ter comprometido os dados pessoais de posse da Riza SEC para a devida apuração. Caso necessário, o Encarregado pelo Tratamento de Dados Pessoais 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 Riza SEC treinará seus Colaboradores sobre a proteção de dados pessoais e de dados sigilosos de acordo com a sua Política de Treinamento e Reciclagem de Colaboradores.

BASE NORMATIVA

As principais normas que fundamentam esta Política incluem:

- Lei nº 12.846/2013.
- Decreto nº 11.129/2022.

Demais normas aplicáveis, conforme atualizações regulatórias.
A Riza SEC reforça a necessidade de monitoramento constante das alterações legislativas e regulatórias pertinentes, bem como da adoção de medidas adequadas sempre que houver atualização normativa, incluindo a revisão desta Política.

APROVAÇÕES

Esta Política foi formalmente aprovada pela Diretora de Compliance da instituição, reforçando o compromisso com as melhores práticas de governança e conformidade regulatória.

Assinado por: Fausto Assis 54D740D765A84CE...

Assinado por: Ifigenia Kalfas E5E933659EF94A0...