



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

ORE INVESTMENTS

ABRIL DE 2025

ÍNDICE

INTRODUÇÃO E OBJETIVO.....	3
PROGRAMA DE SEGURANÇA DA ORE INVESTMENTS.....	4
DESLIGAMENTO DE COLABORADORES.....	13
MONITORAMENTO E TESTES PERIÓDICOS	14
PLANO DE RESPOSTA.....	14
PROTEÇÃO DE DADOS PESSOAIS	15
VIGÊNCIA E ATUALIZAÇÃO	19

INTRODUÇÃO E OBJETIVO

A Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética, 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 Ore Investments, 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 Ore Investments.

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 Ore Investments.

Os sistemas de informação, a infraestrutura tecnológica, os arquivos de dados e as informações internas e externas, são considerados importantes ativos da empresa, uma vez que a Gestora apresenta suas operações dependentes em grande parte da tecnologia para conduzir seus negócios e atender as suas necessidades comerciais e estratégicas.

Portanto, os processos de segurança da informação devem assegurar a integridade, a disponibilidade e a confidencialidade dos ativos da Gestora.

O Diretor de Compliance e a empresa terceirizada de suporte de tecnologia são responsáveis pela implementação do programa de continuidade de negócios e por garantir a segurança da informação e cibernética da Ore Investments.

O Departamento de Compliance é responsável por:

- a) Monitoramento do efetivo trancamento das estações de trabalho;
- b) Monitoramento, juntamente com empresa terceirizada de suporte de tecnologia, da realização de backup das informações arquivadas na Gestora;
- c) Verificação da implementação das regras de acesso e barreiras da informação, assegurando que pastas, diretórios e bases de dados somente sejam acessíveis a pessoas autorizadas;
- d) Verificação do eventual esquecimento de documentos em cima das mesas e/ou nas impressoras;
- e) Coordenação de testes periódicos de segurança, realizados anualmente ou em prazo inferior, caso o Departamento de Compliance julgue necessário, para os sistemas de informações, em especial os mantidos em meio eletrônico e, inclusive, para os fins do plano de continuidade de negócios adotado pela Gestora.

Nesse sentido, é necessário que as informações sejam armazenadas, conduzidas e processadas em ambiente seguro e que todos os usuários da informação compartilhem da responsabilidade pelos

Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética

processos de segurança que foram definidos com a finalidade de se equiparar às boas práticas das organizações nacionais e internacionais.

No âmbito da coordenação e supervisão das diretrizes estabelecidas nesta política, o Departamento de Compliance deverá assegurar que todo o acesso à rede é efetuado com a utilização de usuário e senha.

PROGRAMA DE SEGURANÇA DA ORE INVESTMENTS

(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 integridade 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, 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; 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;

Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética

- 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 Ore Investments pode estar sujeita a mal funcionalidades 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 Ore Investments (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 impactos, considerando aspectos financeiros, operacionais e reputacionais, bem como da probabilidade dos riscos identificados se materializarem.

(ii) Ações de Prevenção e Proteção

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

Deste modo, a Ore Investments 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 Ore Investments teve acesso ou conhecimento por ser de domínio público (“Informação Pública”);

Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética

- 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 Ore Investments;
- operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela Ore Investments; 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 Ore Investments e/ou de seus sócios e clientes.

A partir da definição acima, a Ore Investments 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 Ore Investments:

Estrutura de TI

I. Propriedade dos Recursos de TI

Todos os recursos computacionais e de sistemas disponibilizados para os Colaboradores são de propriedade da Ore Investments. Não é permitida a utilização de notebooks, tablets ou outros hardwares para operações no âmbito da Ore Investments, salvo expressa permissão do Diretor de Risco e Compliance.

II. Disponibilização e uso

Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética

Todos os computadores disponibilizados para os Colaboradores da Ore Investments têm por objetivo o desempenho das atividades profissionais na Ore Investments, 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 pela área responsável, mediante aprovação do Diretor de Risco e Compliance.

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

- A cada novo Colaborador, o Diretor de Risco e Compliance autorizará, mediante solicitação, a criação de novo usuário e a disponibilização técnica de recursos;
- Todos os equipamentos, softwares e permissões acessos devem ser testados, homologados e autorizados pela área responsável, mediante supervisão e aprovação 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, mediante supervisão e aprovação do Diretor de Risco e Compliance;
- A identificação do usuário é feita através do login e senha, que através do registro de logs utilizado pela Ore Investments é sua assinatura eletrônica no servidor da Ore Investments;
- Será apenas permitida senhas com no mínimo 08 (oito) caracteres alfanuméricos, maiúsculos e minúsculos. A 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 Ore Investments, 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 ao Diretor de Risco e Compliance.
- 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 softwares da Ore Investments respeitam as seguintes regras:

- Todos os softwares, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela área responsável, mediante supervisão e aprovação do Diretor de Risco e Compliance;

Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética

- É desabilitado aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada do 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 Ore Investments;
- A utilização de equipamentos pessoais por terceiros nas instalações da Ore Investments e a conexão destes na rede interna à Internet requer autorização prévia e expressa do Diretor de Risco e Compliance. 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 do Diretor de Risco e Compliance.

IV. Registros

A Ore Investments mantém por 5 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.

Nesse sentido, através dos logs realizados pela Ore Investments, 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 Ore Investments.

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 Ore Investments 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;

Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética

- 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 Ore Investments.

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 Ore Investments, este deve sempre resguardar a imagem da Ore Investments, 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 (softwares) 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 Ore Investments;
- 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.

Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética

É proibido o uso de serviços de mensagem instantânea (WhatsApp, Skype etc.), através dos computadores da Ore Investments, exceto em eventuais situações de uso profissional, sendo necessária autorização do Diretor de Risco e Compliance.

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

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 Ore Investments.

IX. Uso de correio eletrônico particular

É proibido a utilização profissional de correio eletrônico particular.

A Ore Investments disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais.

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

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

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 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 Ore Investments, 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 Ore Investments.

XI. Acesso à distância ao e-mail

O usuário pode acessar o seu correio eletrônico cedido pela Ore Investments 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 Ore Investments.

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 Ore Investments.

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 Ore Investments, 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 Ore Investments; e
- Sejam incoerentes com o Código de Ética Corporativa da Ore Investments.

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 Ore Investments é um documento formal e, portanto, possui as mesmas responsabilidades de um documento convencional em papel timbrado da entidade.

Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética

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

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 Ore Investments 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 Ore Investments 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.

Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética

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 Ore Investments:

- (i) Documentos que atestem a existência dos respectivos procedimentos de Cibersegurança;
- (ii) Último relatório de teste/auditoria periódica;
- (iii) As certificações que possam comprovar a devida capacidade técnica do prestador de serviço.

Uma vez recebidos os respectivos documentos, a Área de Compliance 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 pela Ore Investments.

Somente após a aprovação pela Área de Compliance, 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 Ore Investments, 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:

- (i) Software as a Service (SaaS) – utilização do software do provedor por meio de subscrição, eliminando a necessidade de instalação e execução nos computadores;
- (ii) Platform as a Service (PaaS) – desenvolvimento, teste, uso e controle sobre softwares próprios; e
- (iii) 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.

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.

Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética

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 e executados pela área responsável, sob supervisão do Diretor de Risco e Compliance. O referido monitoramento acontecerá de forma contínua, sem periodicidade.

Os Testes de Contingência serão realizados anualmente, de modo a permitir que a Ore Investments 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 Ore Investments.

Ademais, serão realizados Testes Periódicos de Segurança a Ore Investments, 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 Ore Investments, 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 da Ore Investments.

PLANO DE RESPOSTA

Conforme as melhores práticas de mercado, a Ore Investments 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.

Estas providências consistem 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;

Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética

- 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 Ore Investments 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 Ore Investments.

A Ore Investments 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 Ore Investments.

PROTEÇÃO DE DADOS PESSOAIS

Escopo e Abrangência:

Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética

A Ore Investments 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 Ore Investments, 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 Ore Investments.

Importante observar que o escopo da proteção de dados pessoais no âmbito da Ore Investments 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 Ore Investments manteve contato para atender alguma demanda relevante e específica.

Vale ressaltar que todo o tratamento de dados pessoais feito pela Ore Investments 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 Ore Investments 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;

Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética

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 Ore Investments, 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;

Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética

- 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 Ore Investments disponibiliza canal de comunicação, através do endereço dados@ore Investments, 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 Ore Investments, os titulares dos dados (pessoas físicas) e a ANPD.

Período de Armazenamento dos Dados Pessoais:

Os dados pessoais serão armazenados pela Ore Investments 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 Ore Investments 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 Ore Investments, serão notificados sobre tal divulgação, para que tomem as medidas apropriadas.

Adicionalmente, a Ore Investments 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 e dados sigilosos – e aos tratamentos destes, serão apresentadas pelo Encarregado pelo Tratamento de Dados Pessoais para deliberação do Diretor de Gestão de Riscos e de Compliance.

Obrigação de Reporte:

Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética

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 Ore Investments 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 Ore Investments 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.

VIGÊNCIA E ATUALIZAÇÃO

Esta política será revisada anualmente, 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.

CONTROLE DE VERSÕES	DATA	MODIFICADO POR	DESCRIÇÃO DA MUDANÇA
1	Julho/2021	Diretor de Compliance	Versão inicial
2	Julho/2024	RRZ Consultoria	Revisão Periódica
3	Abril/2025	RRZ Consultoria	Reorganização das Políticas e Manuais