POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

EB CAPITAL GESTÃO DE RECURSOS LTDA.

Outubro/2023

INTRODUÇÃO

A presente Política de Segurança da Informação e de Segurança Cibernética ("Política") da EB Capital Gestão de Recursos Ltda. ("EB Capital" ou "Gestora") foi desenvolvida com o objetivo de garantir a proteção e manutenção da privacidade, integridade, disponibilidade e confidencialidade das informações de sua propriedade e/ou sob sua guarda, além de prevenir, detectar e reduzir os riscos relacionados a ocorrência de incidentes cibernéticos.

Em atenção aos dispositivos da Resolução CVM n.º 21/2021 e do Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, assim como à Lei 13.709, de agosto de 2018 ("Lei Geral de Proteção de Dados") a EB Capital 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.

Esta Política demonstra o compromisso da EB Capital em zelar e tratar as informações de seus clientes, colaboradores, fornecedores e parceiros de negócios.

APLICAÇÃO

Esta Política se aplica aos sócios, administradores, funcionários e todos que, de alguma forma, auxiliam o desenvolvimento das atividades da EB Capital ("Colaboradores").

PRINCÍPIOS BASILARES DE SEGURANÇA DA INFORMAÇÃO

Informações são um ativo importante para a EB Capital, por isso nos comprometemos a tratá-las sempre com muita responsabilidade. As atividades da EB Capital e as diretrizes aseguir expostas estão pautadas nos seguintes princípios da segurança da informação:

Confidencialidade: limita o acesso à informação tão somente às pessoas ou instituições autorizadas pelo proprietário da informação;

Integridade: garante a veracidade de dados, que não devem ser alterados enquanto são manipulados, mantendo-se todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudança e garantia do seu ciclo (nascimento, manutenção e destruição);

Disponibilidade: garante que a informação esteja sempre disponível para o uso por usuários autorizados pelo proprietário da informação; e

Valor: a informação deve ter um valor agregado para a Gestora.

DIRETRIZES DE CONFIDENCIALIDADE

Toda classificação de dados deve ser realizada no momento em que a informação for gerada ou, sempre que necessário, em momento posterior. É preciso saber claramente quais são os dados que estão sendo manipulados e o seu propósito, além de garantir a sua proteção. Salvo classificação expressa, todo dado gerado é considerado Público, conforme classificação abaixo.

O nivelamento da classificação aprovado pelo Comitê de *Compliance* e Risco, se apresenta da seguinte maneira:

- Público - todo o conteúdo de todos os documentos é visualizado por qualquer colaborador da EB Capital.

- Restrito - o acesso ao conteúdo é restrito a determinadas pessoas, áreas ou funções dentro da EB Capital.

Grau de Sigilo	Impacto causado pela quebra de confiabilidade
Público	Sem impacto
Restrito	Dano médio ou alto, podendo ou não ocasionar danos à instituição (afetando a imagem, gerar prejuízo financeiro, impactar nas operações e/ou inviabilizar objetivos estratégicos)

Todo tipo de informação escrita, verbal ou apresentada de modo tangível ou intangível, incluindo: know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes, dos clubes, fundos de investimento e carteiras geridas pela Gestora, operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para clubes, fundos de investimento e carteiras geridas pela Gestora, 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 Gestora e a seus sócios ou clientes, independente destas informações estarem contidas em discos, disquetes, pen-drives,fitas, outros tipos de mídia ou em documentos físicos são consideradas Informações Confidenciais.

De modo geral, todas as informações acessadas pelo Colaborador em virtude do desempenho de suas atividades na Gestora, bem como informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, trainees ou estagiários da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral devem ser tratadas como Informações Confidenciais.

Toda e qualquer informação que os Colaboradores tiverem com relação aos clientes ou ex-clientes da EB Capital **deve ser mantida na mais estrita confidencialidade**, **não**

podendo ser divulgada sem o prévio e expresso consentimento do cliente ou ex-cliente, salvo nahipótese de decisão judicial específica que determine à EB Capital a prestação de informações ou, extrajudicialmente, em razão de procedimento fiscalizatório da *Comissão de Valores Mobiliários* ("CVM"). Caso a EB Capital ou qualquer dos Colaboradores sejam obrigados a revelar as informações de clientes em face de procedimento judicial ou extrajudicial da CVM, tal fato deve ser seguido de imediata e expressa comunicação aos clientes afetados, caso não haja norma dispondo de forma diversa.

Os Colaboradores devem envidar seus melhores esforços para garantir que os prestadores de serviços que porventura venham a trabalhar junto à EB Capital, tais como, instituições administradoras de fundos de investimento, distribuidores de títulos e valores mobiliários, escritórios de advocacia, corretores, agentes autônomos, entre outros, mantenham a confidencialidade das informações apresentadas, sejam tais informações dos clientes ou das operações realizadas pela EB Capital. Neste sentido, qualquer conduta suspeita deve ser informada imediatamente e por escrito ao(à) Diretor(a) de Compliance, Gestão de Risco e PLD e/ou à administração da EB Capital, para que sejam tomadas as medidas cabíveis. Além disso, confidencialidade das informações deve ser mantida durante e mesmo após o fim do contrato com clientes e terceiros.

A EB Capital exige que seus Colaboradores atuem buscando a garantia da confidencialidade das informações às quais tiverem acesso. Assim, é recomendável que os Colaboradores não falem a respeito de informações obtidas no trabalho em ambientes públicos, ou mesmo nas áreas comuns das dependências da EB Capital, e que tomem as devidas precauções para que as conversas por telefone se mantenham em sigilo e não sejam ouvidas por terceiros.

É terminantemente proibido fazer cópias (físicas ou eletrônicas) ou imprimir os arquivos utilizados, gerados ou disponíveis na rede da Gestora e circular em ambientes externos à Gestora com estes arquivos (físicos ou eletrônicos) sem a devida autorização, uma vez que tais arquivos contêm informações que são consideradas como Informações Confidenciais.

Além disso, a Gestora poderá gravar qualquer ligação telefônica realizada ou recebida por meio das linhas telefônicas disponibilizadas pela Gestora para as atividades profissionais dos Colaboradores.

Todo e qualquer material com informações de clientes ou de suas operações deverá ser mantido nas dependências da EB Capital, sendo proibida a cópia ou reprodução de tais materiais, salvo mediante autorização expressa do superior hierárquico do Colaborador. Ainda, todo e qualquer arquivo eletrônico recebido ou gerado pelo Colaborador no exercício de suas atividades deve ser salvo no diretório exclusivo do cliente ou do projeto a que se refere tal arquivo eletrônico.

A EB Capital é comprometida em atender os requisitos da Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) e alterações posteriores, bem como demais regulamentação relacionada à privacidade de informação de seus clientes, protegendo essas informações e não as compartilhando indevidamente ou utilizando-as para obter vantagens próprias ou indevidas. Para maiores informações, verificar a Política de Privacidade da EB Capital.

DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

A. Aspectos gerais

A EB Capital possui sistema de controle de acesso de pessoas autorizadas às dependências do escritório por cartões magnéticos e/ou leitura facial com possibilidade de utilização de logs e histórico de acesso e/ou identificação por meio de digitais.

No que diz respeito à infraestrutura tecnológica, destacamos que todas as informações, sejam dos clientes ou das operações a eles relacionadas, ficam armazenadas em serviços de armazenamento de dados na nuvem (*cloud computing*).

A realização de *back up* de todas as informações armazenadas na nuvem é total a cada 6 (seis) meses e incremental a cada 2 (dois) dias, sendo uma cópia mantida na nuvem e outra em nosso servidor local, com vistas a evitar a perda de informações, e viabilizando sua recuperação em situações de contingência.

A Gestora conta com empresas contratadas especializadas no tema de segurança cibernética, atuando na prevenção, monitoramento e mitigação de riscos cibernéticos aos quais a EB Capital esteja exposta.

O acesso aos sistemas de informação da EB Capital é feito por meio de um par "usuário/senha" que permite que seja acompanhado, de forma precisa, as atividades desenvolvidas por cada um dos Colaboradores. O acesso e o uso de qualquer informaçãopelo usuário devem se restringir ao necessário para o desempenho de suas atividades profissionais no âmbito da Gestora. O controle desses dados é de domínio da EB Capital,uma vez que o armazenamento dos dados ocorre na nuvem, porém com acesso restrito aosColaboradores da EB Capital, garantindo, assim, a confidencialidade e confiabilidade da informação.

Para acessar informações nos sistemas da Gestora deverão ser utilizadas somente ferramentas e tecnologias autorizadas e previamente estabelecidas pela EB Capital, de forma a permitir a identificação e rastreamento de quais usuários tiveram acesso a determinadas informações (os logs de acesso ficam armazenados nos sistemas).

Adicionalmente, informamos que a rede da EB Capital é composta por dois tipos de acesso: (i) pessoal, onde somente o usuário visualiza o conteúdo e (ii) compartilhado, onde os arquivos pertencem a um diretório de propriedade exclusiva do administrador do domínio da EB Capital e os acessos aos usuários são liberados conforme solicitação dos *Partners* e *Principals* da Gestora.

Todo Colaborador que tiver acesso aos sistemas de informação da EB Capital é responsável por tomar as precauções necessárias a fim de impedir o acesso não autorizado aos sistemas. O Colaborador deve manter em local seguro suas senhas e outros meios de acesso aos sistemas, e não as divulgar a terceiros em qualquer hipótese.

Os acessos acima referidos são imediatamente cancelados em caso de desligamento do Colaborador da Gestora.

A EB Capital se reserva o direito de proibir o uso de telefones celulares na área de gestão ede rastrear, monitorar, gravar e inspecionar todo e qualquer tráfego de voz realizado por meio de contato telefônico e internet, bem como troca de informações escritas transmitidas via internet, ou mesmo intranet, sistema de mensagem instantânea, fax, correio físico e eletrônico (e-mail), e ainda, como os arquivos armazenados ou criados pelos recursos da informática pertencentes à EB Capital ou utilizados em nome dela, a fim de assegurar o fiel cumprimento desta Política, bem como da legislação em vigor.

B. Identificação e avaliação de riscos

A EB CAPITAL entende que o gerenciamento dos riscos em segurança da informação é um processo cíclico e dinâmico que requer uma constante participação de todas as pessoas. Devido ao fato de ser um processo cíclico, está em constante evolução e aprimoramento mediante a comparação dos resultados do processo com os resultados esperados e realização de ajustes para melhorar os resultados.

O processo de gerenciamento do risco está baseado nas seguintes etapas:

- Identificação dos ativos críticos;
- Levantamento e avaliação dos riscos associados a esses ativos;
- Criação de um plano para o tratamento desses riscos; e
- Execução do plano de tratamento de riscos.

O processo é cíclico, no sentido de que, após a execução do plano de tratamento de riscos, o novo nível de risco deve ser comparado com o nível avaliado inicialmente. A informação resultante dessa comparação deve ser utilizada para iniciar novamente o processo.

O processo é dinâmico também no sentido de que os ativos críticos de informação mudam ao longo do tempo e, portanto, devem ser avaliados periodicamente para manter a sua identificação atualizada com os processos de negócio.

Assim, a EB identifica e avalia periodicamente os principais riscos cibernéticos aos quais está exposta. O Guia de Cibersegurança da *Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais* ("Anbima") definiu que os ataques mais comuns de criminosos cibernéticos são os seguintes:

(i) Malware: softwares desenvolvidos para corromper computadores e redes:
   a) *vírus*: software que causa danos a máquina, rede, softwares e banco de dados;
   b) *cavalo de Troia*: aparece dentro de outro software e cria uma porta para a invasão do computador;
   c) *spyware*: software malicioso para coletar e monitorar o uso de informações;
   d) *ransomware*: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

(ii) Engenharia social: métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:

a) *pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;

b) *phishing*: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;

c) *vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;

d) *smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e

e) 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.

(iii) 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;

(iv) Invasões (*advanced persistent threats*): ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

C. Ações de prevenção

Para fins de manutenção das Informações Confidenciais, a EB Capital recomenda que seus Colaboradores (i) bloqueiem o computador quando esse não estiver sendo utilizado; (ii) mantenham anotações, materiais de trabalho e outros materiais semelhantes sempre trancados em local seguro; (iii) descartem materiais usados, destruindo-os fisicamente e (iv) jamais revelem a senha de acesso aos computadores ou sistemas eletrônicos, de preferência modificando-as periodicamente.

O controle da informação transmitida por meio dessas ferramentas é essencial. Para tanto, algumas regras especificas sobre a segurança da informação requerem atenção especial, pois visam a proteção das informações de clientes e da Gestora, evitando o risco de revelação ou alteração por pessoas não autorizadas. Os sistemas de e-mail e outros dispositivos de comunicação fornecidos pela EB Capital são de propriedade da EB Capital.

São <u>proibidas</u>:

(i) mensagens que violam nossa política contra a oferta e convites à participação de atividades ilegais, como apostas ou o uso e venda de substâncias controladas; e

(ii) declarações que, se feitas em quaisquer outros fóruns, violariam qualquer ponto

de nossas políticas, incluindo as políticas contra abuso ou discriminação e a má-utilização de informações confidenciais.

Sujeita às leis e regulamentos aplicáveis, a EB Capital se reserva o direito de monitorar, analisar e expor o acesso à Internet e ao e-mail, se julgar apropriado.

Sempre efetue *logoff* de todos os sistemas acessados ao término da utilização.

1. Senhas

As senhas de acesso à rede e sistemas da EB Capital devem ser trocadas pelos Colaboradores com frequência. Caso desconfie que sua senha não seja mais segura, recomendamos sua mudança mesmo antes do prazo de validade determinado. Sua senha não deve ser jamais revelada a ninguém, nem mesmo para o Responsável de Tecnologia da Informação ("TI").

Não relacione suas senhas a informações pessoais, como nome de usuário, nome de algum membro da família, departamento, time de futebol etc., e não adote a mesma senha para mais de um aplicativo.

Não recomendamos o uso de recursos fornecidos por softwares que permitem o armazenamento de senhas.

Caso identifique alguma mensagem suspeita solicitando a troca da sua senha, seja por e-mail, seja pela tela do seu computador, verifique com o responsável pelo TI a veracidade da solicitação antes de realizar os procedimentos de troca.

Qualquer ato executado com seu nome de usuário e senha será de sua inteira responsabilidade, por isso, tome todas as precauções para que essas informações permaneçam secretas.

2. E-mails

Nossos servidores de e-mail encontram-se protegidos contra vírus e códigos maliciosos, porém, algumas atitudes do usuário são necessárias para contribuir com a segurança da informação:

(i) Não abra em hipótese alguma anexos com as extensões ".bat", ".exe", ".src", ".lnk" e ".com";

(ii) Não utilize contas pessoais para comunicar-se com clientes ou para transmitir qualquer tipo de informação confidencial ou interna;

(iii) Ao trocar e-mails com clientes e parceiros, o conteúdo das mensagens poderá ser considerado posição oficial da EB Capital, portanto, aja com seriedade e profissionalismo.

(iv) Não envie mensagens internas ou externas que possam prejudicar a imagem da EB Capital, como piadas, material de caráter sexual, imagens, vídeos (com extensões .mpeg, .avi ou outras), músicas (com extensões .mp3, .wav ou outras), jogos,

mensagens ou textos de conteúdo religioso, criminoso, político ou que possa ser interpretado como ofensivo;

(v) Ao receber e-mails com links, verifique se ele corresponde ao endereço que aparece na tela. Para tanto, posicione o ponteiro do mouse sobre o link (não clique).Se o endereço exibido não for o mencionado, não acesse o link;

(vi) Desconfie de todos os e-mails com assuntos estranhos;

(vii) Não crie nem passe adiante correntes nas quais o receptor é induzido a enviar mensagens para outros sem que haja necessidade profissional;

(viii) Não leia, acesse nem divulgue e-mails de outros colaboradores, clientes e prestadores de serviço sem a devida autorização;

(ix) Evite utilizar o e-mail da empresa para assuntos pessoais;

(x) Se o espaço utilizado pelo Mailbox ultrapassar 400 MB, o usuário ficará impossibilitado de enviar mensagens até que o conteúdo seja reduzido;

(xi) Evite anexos muito grandes;

(xii) Procure limpar constantemente pastas como *Deleted Items* e *Sent Items*.

E-mails pessoais

As contas pessoais de e-mail baseadas na Internet (ex.: Gmail, Hotmail, Yahoo, Aol) somente devem ser utilizadas pelos integrantes da EB Capital para fins pessoais, sendo proibido o uso de tais contas para conduzir qualquer atividade relacionada à Gestora.

3. Internet

Ao utilizar a conexão de internet da Instituição é proibido:

(i) Acessar sites com conteúdo pornográfico, jogos, bate-papo, apostas, vídeos (ex.: *You Tube*) e de relacionamento (ex.: *Facebook*, *Twitter*);

(ii) Usar softwares P2P (*kazaa*, *Morpheus*, *Emule*, etc.);

(iii) Acessar sites de FTP sem autorização do Responsável de TI;

(iv) O uso de IM (*instant messengers*);

(v) Fazer download ou upload de softwares ou dados não legalizados;

(vi) Usar serviços de streaming como rádios *on-line* etc.;

(vii) Usar discos virtuais para armazenamento externo de dados da EB Capital;

(viii) Utilizar informações classificadas como confidenciais ou internas em sites pessoais, blogs ou qualquer outro meio de publicação na Internet;

(ix) Navegar na Internet em sites não confiáveis (como os de pornografia, "hackeismo", dinheiro fácil etc.);

(x) Fazer download de arquivos não relacionados ao trabalho.

Somente é permitida a navegação convencional. Casos específicos que exijam outros protocolos devem ser solicitados para o responsável de TI e estarão sujeitos à autorizaçãodo supervisor imediato e/ou do diretor responsável.

Somente funcionários com autorização podem baixar programas diretamente relacionados às atividades da Gestora, e devem providenciar o que for necessário para obtenção de licença e

registro desses programas. Referidos funcionários terão permissão específica em seu usuário para realizar tal atividade.

A EB Capital pode gerar relatórios dos sites acessados, e caso julgue necessário poderá bloquear o acesso a arquivos/domínios que comprometam o uso de banda ou prejudiquemo bom andamento dos trabalhos.

A EB Capital monitora todos os acessos à Internet. Portanto, utilize sua infraestrutura de acesso com bom senso e moderação.

4. Redes Sociais

Da mesma forma adotada para contas de e-mail pessoal, as plataformas de redes sociais (ex.: *Facebook*, *Twitter*, *Instagram*) somente devem ser utilizadas pelos integrantes da EB Capital para fins pessoais, sendo proibido o uso de tais contas para conduzir qualquer atividade relacionada à Gestora.

Somente integrantes autorizados podem emitir qualquer opinião ou fazer comentários em mídias sociais com relação à Gestora e suas atividades.

5. Rede

É proibido acessar a rede da EB Capital para:

(i) tentar acesso não autorizado aos servidores;
(ii) colocar em prova a segurança da rede;
(iii) tentar fraudar autenticação de usuários;
(iv) interferir nas atividades de outros usuários, alterando arquivos que não sejam de sua propriedade;
(v) expor, armazenar, distribuir, editar ou gravar material de natureza pornográfica e racista por meio do uso dos recursos da Gestora;
(vi) configurar contas de e-mail particulares.

É proibido acessar drives de rede de outras áreas sem autorização.

O diretório pessoal deve ser periodicamente revisto, evitando o acúmulo de arquivos inúteis. Computadores particulares ou de visitantes não devem ser plugados nos pontos de rede.

É proibido armazenar na rede arquivos de música, vídeos e fotos que não sejam de propriedade da Gestora. Arquivos desse tipo serão apagados sem aviso prévio.

Cópias de arquivos da rede para dispositivos externos (CDs, DVDs) devem ser solicitadas ao responsável de TI e serão executadas apenas com autorização do responsável pela área.

Acessos remotos à rede da Gestora devem ser autorizados pelo responsável da área de TI e não devem ser utilizados para a realização de download de arquivos ou documentos da EB

Capital.

6. Trabalho Remoto

De acordo com as permissões estabelecidas pela EB Capital, no caso de Colaboradores trabalhando de forma remota, é proibida a gravação, transmissão e/ou manutenção de arquivos de propriedade da EB Capital em computadores pessoais.

D. Testes periódicos

Periodicamente, a Gestora realiza testes de segurança em todo o seu sistema de informação. Dentre as medidas, incluem-se, mas não se limitam:

(i) Verificação do login dos Colaboradores;
(ii) Testes no firewall;
(iii) Testes nas restrições impostas aos diretórios;
(iv) Manutenção periódica de todo o "hardware" pelo responsável de TI da Gestora;
(v) Testes no "back-up" (salvamento de informações), realizado em nossa nuvem.

E. Plano de resposta

Não obstante todos os procedimentos e aparato tecnológico robustos adotados pela Gestora para preservar o sigilo das informações confidenciais, reservadas ou privilegiadas, na eventualidade de ocorrer o vazamento de quaisquer informações, ainda que de forma involuntária, o(a) Diretor(a) de *Compliance*, Gestão de Risco e PLD deverá tomar ciência do fato tão logo seja possível.

De posse da respectiva informação, o(a) Diretor(a) de Compliance, Gestão de Risco e PLD, primeiramente, identificará se a informação vazada se refere ao fundo de investimento gerido ou aos dados pessoais de cotistas. Realizada a identificação, o(a) Diretor(a) de *Compliance*, Gestão de Risco e PLD procederá da seguinte forma:

1. <u>No caso de vazamento de informações relativas aos fundos de investimento geridos</u>

Imediatamente, seguirá com o rito para publicação de fato relevante, nos termos da regulamentação vigente, a fim de garantir a ampla disseminação e tratamento equânime da informação. Esse procedimento visa assegurar que nenhuma pessoa seja beneficiada pela detenção ou uso da informação confidencial, reservada ou privilegiada atinente ao fundo de investimento.

2. <u>No caso de vazamento de informações relativas aos cotistas</u>

Neste caso, o(a) Diretor(a) de *Compliance*, Gestão de Risco e PLD procederá com o tanto necessário para cessar a disseminação da informação ou atenuar os seus impactos, conforme o caso. Para tanto, poderá, dentre outras medidas: (i) autorizar a contratação de empresa especializada em consultoria para proteção de dados; (ii) autorizar a contratação de advogados especializados na matéria; (iii) entrar em contato com os responsáveis pelo(s)

veículo(s) disseminador(es) da informação. Sem prejuízo, o(a) Diretor(a) de *Compliance*, Gestão de Risco e PLD ficará à inteira disposição para auxiliar na solução da questão. Ademais, será providenciada a comunicação do incidente à Autoridade Nacional de Proteção de Dados (ANPD), bem como aos cotistas envolvidos.

Após a execução do Plano de Resposta ao incidente identificado, a EB Capital providenciará uma análise crítica de caso para identificação e reavaliação de riscos e oportunidades de melhoria em seus processos, para evitar novas ocorrência, providenciando a implementação dos planos de ação cabíveis visando o fortalecimento do ambiente de controles internos da Gestora.

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.

CONTINUIDADE DOS NEGÓCIOS

A. Objetivo

Com o objetivo de assegurar a continuidade dos negócios em eventos que impliquem na impossibilidade da operação normal em suas instalações principais, a EB Capital possui uma série de medidas e procedimentos, incluindo as atribuições e responsabilidades de cada Colaborador na execução do Plano de Continuidade de Negócio ("PCN").

O PCN é um plano traçado para que seja possível dar continuidade à execução de atividades consideradas críticas para a prestação de serviços pela EB Capital, de forma que os interesses dos clientes da EB Capital não sejam prejudicados.

B. Principais contingências mapeadas e respostas do PCN

A Gestora trabalha com todos os seus dados na nuvem (OneDrive Microsoft), possibilitando o acesso aos arquivos de forma segura mesmo não estando fisicamente no escritório.

De forma a se prevenir da maneira mais adequada, a EB Capital adotará os seguintes mecanismos de resposta para cada contingência específica:

Queda de energia.

Temos *no break* com autonomia de 30 minutos. O edifício em que nossa sede fica localizada possui gerador a gás de rua com autonomia ilimitada e em caso de defeito nos geradores agás, há geradores a diesel também com autonomia ilimitada.

Procedimento de Ativação: Constatada a queda de energia e, caso o *no break* não seja acionado automaticamente, o(a) Diretor(a) de Compliance, Gestão de Risco e PLD deverá determinar

oacionamento manual, a fim de garantir a manutenção das atividades da Gestora e a proteção das informações e tecnologias.

Prazo para Ativação: O *no break* deverá ser acionado, automaticamente, e de forma imediata, ou, manualmente, dentro do prazo de até 60 (sessenta) minutos após a queda de energia.

Queda do link para acesso à internet.

Dois links redundantes para acesso à internet. Caso os dois links de internet fiquem inoperantes, há a possibilidade de cada usuário rotear a internet do celular ou ir a qualquer outro lugar com internet (residência, co-works, etc).

Procedimento de Ativação: No caso de queda do link para acesso à internet, o(a) Diretor(a) de *Compliance*, Gestão de Risco e PLD deverá estabelecer a migração para o link de outra operadora em funcionamento, caso esta não ocorra de forma automática. Com esse procedimento, garante-se o regular exercício das atividades dos Colaboradores.

Prazo para Ativação: Tão logo o(a) Diretor(a) de *Compliance*, Gestão de Risco e PLD tome ciência do fato, deverá proceder com o tanto necessário para viabilizar a migração.

Contingências para e-mail.

Serviço de e-mail é hospedado em nuvem, garantindo a continuidade do acesso remoto. Há possibilidade de comunicação nos celulares dos funcionários.

Contingências com serviço de telefonia e problemas com central de telefonia.

Em caso de indisponibilidade da linha telefônica por problema da operadora ou central, aEB Capital autoriza o Colaborador a fazer uso do seu aparelho de celular.

Procedimento de Ativação: Identificadas contingências com o serviço de telefonia ou problemas com a central, o(a) Diretor(a) de *Compliance*, Gestão de Risco e PLD deverá comunicar os Colaboradores sobre o ocorrido e orientá-los a fazer uso de seu aparelho celular até que o serviço seja reestabelecido.

Prazo para Ativação: Imediatamente após o(a) Diretor(a) de *Compliance*, Gestão de Risco e PLD tomar ciência do fato.

Contingências com CPU.

Equipamento reserva e acesso remoto aos diretórios e arquivos na nuvem.

Procedimento de Ativação: No caso de contingência com alguma CPU, o Colaborador que faz uso da máquina afetada deverá informar o fato à TI e, até sua regularização, utilizar equipamentos reserva que estão à disposição na sede da Gestora.

Prazo para Ativação: O Colaborador deverá tomar as providências acima em até 60 (sessenta) minutos após a contingência ocorrida com sua CPU.

Invasão da intranet por hackers.

Firewall com monitoramento e alertas de segurança. São, ainda, realizados "pentests" (testes de penetração) periódicos.

CANAL CONFIDENCIAL

O desconhecimento em relação a qualquer das obrigações e compromissos decorrentes deste documento não justifica desvios, portanto, em caso de dúvidas ou necessidade de esclarecimentos adicionais sobre seu conteúdo, favor contatar o(a) Diretor(a) de *Compliance*, Gestão de Risco e PLD, por meio do e-mail compliance@ebcapital.com.br.

Violações ou suspeitas de violação devem ser reportadas no Canal Confidencial da EB Capital, disponível no site www.canalconfidencial.com.br/ebcapital. Todo e qualquer reporte será tratado de forma anônima e confidencial, sendo terminantemente proibida qualquer retaliação contra qualquer denunciante de boa-fé.

Quando constatada a violação, o Colaborador infrator estará sujeito às medidas disciplinares.

MONITORAMENTO E AÇÕES DE COMUNICAÇÃO E TREINAMENTO

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 EB Capital ao Colaborador.

A EB Capital deverá manter o programa de segurança da informação continuamente atualizado, identificando novos riscos, ativos e processos, reavaliando os riscos residuais e, se o caso, atualizando esta Política.

Também realizará ações de comunicação e treinamento para capacitação e conscientização dos Colaboradores, para que todos tenham as habilidades necessárias para proteger as informações como parte de suas responsabilidades.

ATUALIZAÇÃO DESTA POLÍTICA

Esta Política deve ser revisada e atualizada pelo(a) Diretor(a) de *Compliance*, Risco e PLD em conjunto com o Responsável de TI a cada 24 (vinte e quatro) meses ou sempre que novos riscos e mitigadores forem identificados.