Safari
capital

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

SAFARI CAPITAL GESTÃO DE RECURSOS LTDA.

Safari
capital

1. APRESENTAÇÃO

A Política de Segurança da Informação da Safari Capital ("Safari"), aplica-se a todos os sócios, Colaboradores, prestadores de serviços, sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Safari, ou que acesse informações a ela pertencentes. Todo e qualquer usuário com acesso computadorizado ou digital nesta instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

OBJETIVOS

A Política de Segurança da Informação da Safari visa proteger as informações de sua propriedade e/ou sob sua guarda, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas.

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

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

Safari
capital

SEGURANÇA DE INFORMAÇÕES E CIBERNÉTICA

As medidas de segurança utilizadas pela Safari têm por finalidade minimizar as ameaças ao patrimônio, à imagem e aos negócios da empresa.

É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis da Safari e circulem com eles em ambientes externos à empresa, sem prévia autorização do Diretor de Riscos e *Compliance*. Informações de caráter sensível ou confidencial da empresa ou de clientes deverão ser armazenadas em diretórios de rede com acesso restrito, e controlado pela equipe de Riscos e *Compliance* da Safari.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Safari. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade. Ainda, qualquer impressão de documentos deve ser prontamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno da Safari.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso, de maneira a evitar sua recuperação, sendo recomendável o seu descarte total.

Adicionalmente, os Colaboradores devem se abster de utilizar pen-drives, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Safari.

É proibida a conexão de equipamentos na rede da Safari que não estejam previamente autorizados. Novos equipamentos e/ou sistemas deverão ter suas configurações feitas pela "equipe de TI" (empresa terceirizada contratada pela Safari para prover serviços de suporte em informática e afins).

Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade devendo observar também, quando aplicável (a depender da natureza da Informação armazenada), a Política de Privacidade de Dados da Safari (Anexo I à presente Política), bem como as disposições na Lei nº 13.709/18 (Lei Geral de Proteção de Dados – LGPD) e regulamentações.

O acesso a sites e blogs, bem como o envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo também é terminantemente proibido, como também o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da Safari.

Não é permitida a instalação de software nos equipamentos por qualquer usuário, exceto pelas pessoas chaves descritas no Plano de Contingência abaixo ou pela equipe de TI terceirizada.

Todo conteúdo que está na rede pode ser acessado pelos Administradores da Safari ou pelo Diretor de Riscos e *Compliance* , inclusive e-mails. Arquivos pessoais salvos em cada computador poderão ser acessados. A confidencialidade dessas informações deve ser respeitada, e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais, ou em atendimento às determinações judiciais ou administrativas. O acesso à rede é restrito e baseado na liberação definida previamente.

Safari
capital

Por fim, convém ressaltar que a Safari conta com sistemas e ferramentas contratados para arquivamento (rede), *firewall*, antivírus, *backup*, prevenção de invasão e linha de contingência.

SERVIÇOS DE REDE

As redes de serviços são segmentadas para garantir a segurança e desempenho entre elas. Está implantado um sistema de prevenção de invasão na rede e nos equipamentos para garantir a segurança da informação e disponiblidade de serviços.

ARMAZENAMENTO DE DADOS

O armazenamento de dados (backup) é realizado diariamente em cloud e localmente sendo disponível para *restore* após liberação do responsável de segurança da informação.

INSTALAÇÕES FíSICAS TECNOLOGIA / ACESSO FÍSICO

Para garantir o ambiente com alta disponibilidade está implantado um *nobreak* central para assegurar problemas de energia até a entrada do gerador. O sistema de ar condicionado está implantado no CPD. O acesso físico ao CPD é controlado. Está previamente autorizado somente o acesso de pessoas da equipe de TI e de pessoas chaves da Safari previamente definidas .

INDISPONIBILIDADE DE ACESSO À INFORMAÇÃO

Em caso de problemas de indisponibilidade de acesso à informação, é acionado o processo de plano de contingência de crises sendo avaliado o impacto sobre o negócio.

Safari
capital

TREINAMENTO

A Safari entende essencial que o seu treinamento anual, supervisionado pelo Diretor de Riscos e *Compliance*, abranja os preceitos contidos na presente política, de modo que seus Colaboradores estejam sempre cientes e em consonância com os procedimentos de segregação e segurança das informações.

RELATÓRIO DE TESTES DE SEGURANÇA DAS INFORMAÇÕES

Anualmente ou quando necessário, a Safari, por meio da equipe de TI terceirizada, realizará testes dos seus sistemas de segurança de informações, bem como dos preceitos contidos na presente política, incluindo, mas não se limitando, os procedimentos de descarte de informações pelos Colaboradores, individualização dos usuários, dentre outros.

Os resultados desses testes, bem como os procedimentos para saneamento de eventuais problemas, serão descritos em Relatório próprio emitido pela equipe de suporte de TI .

Os testes serão realizados pela equipe de suporte de TI contratada ou sob a sua supervisão, e buscarão cobrir os seguintes pontos:

a) identificação e avaliação de potenciais riscos cibernéticos, envolvendo ativos de hardware e software, além de processos que necessitem de proteção;

b) estabelecimento de medidas de prevenção e mitigação de riscos identificados na atividade, de forma a buscar evitar eventuais ataques cibernéticos aos dados e equipamentos da empresa;

c) detecção de possíveis anomalias e/ ou fragilidades no ambiente tecnológico, incluindo acessos não permitidos, usuários não cadastrados, e dispositivos não autorizados;

O plano de resposta e recuperação de incidentes deve ser elaborado em conjunto entre as áreas internas de Riscos e Compliance, e da empresa de TI contratada. O plano identificará papéis e responsabilidades, com previsão de acionamento de colaboradores e contatos externos.

As documentações relacionadas aos planos definidos e testes realizados, assim como os resultados auferidos e ações corretivas e mitigantes, deverão ser mantidas em diretório interno da área de Riscos e Compliance como evidência em eventuais questionamentos internos ou de órgãos reguladores ou auto-reguladores.

Os temas relacionados à segurança da informação e cibernética serão tratados no Comitê de Riscos e *Compliance*, de forma ordinária, ou mesmo em reunião específica, em casos de eventos extraordinários, para que sejam tomadas de forma tempestiva medidas de recuperação, limitação de danos, e resposta relevante.

PLANO DE CONTINGÊNCIA DE CRISES

A SAFARI tem um *nobreak* que suporta a operação entre 2 e 3 horas (a depender da quantidade de acessos no momento do incidente) em caso de problemas de fornecimento de energia, além dos geradores do condomínio da sua sede.

Todos os servidores são instalados em Cloud de alta disponibilidade que podem ser acessados em qualquer local com acesso à internet.

Em caso de problemas de energia não suportados pelo gerador, ou qualquer outro imprevisto ou acontecimento que impeça o acesso às instalações físicas da SAFARI CAPITAL, há máquina virtual no cloud da Microsoft para utilização em casos de contingência, que é destinada a assegurar a continuidade regular dos negócios.

As pessoas chaves da Safari para tratar casos de contingências são, em ordem de importância, o *trader* operador da equipe de gestão e o Diretor de Administração de Carteiras todos com conhecimento para acessar os sistemas remotos e manter as atividades essenciais da Safari em andamento até a recuperação das instalações físicas necessárias.

VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada anualmente e uma nova versão será elaborada quando for identificada a necessidade de atualização do seu conteúdo.

É parte integrante da presente política de Segurança da Informação e Cibernética o Anexo I que contém a Política de Privacidade de Dados da Safari.

Safari
capital

ANEXO I

Política de Privacidade de Dados

Safari
capital

1. CONSIDERAÇÕES INICIAIS

A Safari Capital Gestão de Recursos Ltda. (Controlador), na condição de Controladora de dados pessoais para fins da Lei nº 13.709/18 (Lei Geral de Proteção de Dados - LGPD), formaliza a presente política como forma de demonstrar o seu comprometimento e transparência, perante todos os titulares de dados pessoais, na busca pelo adequado tratamento dos dados de pessoas naturais que porventura venha a ter acesso no âmbito de suas atividades e responsabilidades.

Dessa forma, com base nas políticas e diretrizes internas do Controlador e da legislação de proteção de dados vigente, os dados pessoais de pessoas naturais que porventura sejam fornecidos ao Controlador serão objeto de adequado tratamento interno sujeitando-se à confidencialidade e à política de segurança da informação e cibernética do Controlador que já devem ser observadas por todos os seus colaboradores.

2. CONCEITOS

Para fins da presente política, os termos abaixo devem ser interpretados da seguinte forma:

- “Controlador”: a pessoa natural ou jurídica responsável pelas decisões referentes ao Tratamento de Dados Pessoais;

- “Operador”: a pessoa natural ou jurídica que realiza o Tratamento de Dados Pessoais em nome do Controlador, seguindo as suas instruções;

- “Agentes de tratamento”: o controlador e o operador;

- “Titular”: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

- “Dados Pessoais”: informações relacionadas à pessoa natural identificada ou identificável;

- “Dado anonimizado”: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

– “Tratamento”: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

- “Anonimização”: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

- “Consentimento”: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

- “Encarregado”: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)

- “Usuário”: pessoa natural que acessa o site do Controlador.

3. UTILIZAÇÃO DE COOKIES

Cookies são pequenos arquivos que ficam gravados no computador do usuário do site sendo que, através deles, é possível obter informações sobre a navegação do usuário.

O site do Controlador contém cookies que têm por finalidade melhorar a experiência de quem o acessa.

Os cookies utilizados recolhem informações estatísticas sobre a forma como os usuários utilizam esse site, permitindo ao Controlador aperfeiçoar o seu funcionamento e melhorar a experiência de quem o acessa. Tais informações, no entanto, não identificam diretamente o usuário.

O site do Controlador pode, no entanto, conter links para site de terceiros, sobre os quais o Controlador não tem qualquer responsabilidade.

É possível ao usuário desativar os cookies do seu computador mediante configuração específica em seu navegador o que, no entanto, poderá prejudicar/inviabilizar a experiência de navegação do usuário no site do Controlador. Para saber como desativar tal função, o usuário pode acessar as opções de ajuda de seu navegador.

Safari
capital

4. DADOS PESSOAIS COLETADOS

Para fins de coleta de dados, a presente política tem duas categorias:

a) Dados de terceiros; e

b) Dados de colaboradores (CLT ou sócios diretos ou indiretos) do Controlador.

Em relação ao item a) o Controlador poderá, eventualmente, ter acesso aos seguintes dados pessoais de titulares:

- Nome
- e-mail
- data de nascimento
- RG
- CPF
-telefone
- cônjuge
- domicilio
- profissão

Em relação ao item b), o Controlador poderá coletar os seguintes dados pessoais de titulares:

- Nome
- Data de Nascimento
- Nome dos genitores
- RG
- CPF
- CNH
- Título de eleitor
- Imagem
- Estado civil
- Nível de instrução ou escolaridade
- Profissão
- Currículo profissional
- Endereço residencial
- Telefone
- E-mail
- Biometria
- Dados bancários

Safari
capital

5. FINALIDADE DO TRATAMENTO DOS DADOS

Os dados pessoais de terceiros poderão ser utilizados para envio de e-mails de divulgação do Controlador. Além disso, em situações excepcionais, eles também poderão ser utilizados quando cabíveis no contexto operacional em que se insere o serviço do Controlador.

Em relação aos dados pessoais dos colaboradores, estes serão utilizados dentro da finalidade que a relação laboral ou societária estabelecida entre os colaboradores e o Controlador demanda e o contexto de mercado regulado que o Controlador atua. Dessa forma, a finalidade do tratamento de dados pessoais de colaboradores tem como intuito viabilizar tanto o devido cumprimento das políticas internas do Controlador, quanto demandas comerciais, *due diligences* de parceiros comerciais e também o cumprimento das regras trabalhistas, societárias, contábeis regulatórias, dentre outras, a que o Controlador está sujeito.

6. COMPARTILHAMENTO DE DADOS

Em regra, o Controlador não compartilha dados pessoais do Titular com terceiros que não sejam autorizados pelo Titular ou no contexto de seus serviços.

Eventual transferência de dados não autorizados está restrita aos casos previstos na legislação vigente de proteção de dados, sendo que tanto o Controlador quanto o Operador se comprometem com o integral atendimento aos requisitos legais estabelecidos na legislação de tratamento de dados.

7. SEGURANÇA DOS DADOS

O Controlador responsabiliza-se pela manutenção de medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

Cada Colaborador do Controlador, no escopo de sua atividade, deve zelar pela segurança dos dados pessoais de titulares que porventura tenha acesso nos termos desta política e da Lei nº 13.709/18.

Em conformidade ao art. 48 da Lei nº 13.709/18, o Controlador comunicará ao Titular e à Autoridade Nacional de Proteção de Dados (ANPD) a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante ao Titular.

Safari
capital

8. TÉRMINO DO TRATAMENTO DOS DADOS

O Controlador poderá manter e tratar os dados pessoais do Titular durante todo o período em que estes forem pertinentes ao alcance das finalidades listadas nesta Política.

Dados pessoais anonimizados, sem possibilidade de associação ao indivíduo, poderão ser mantidos por período indefinido.

O Titular poderá solicitar via e-mail (ouvidoria@safaricapital.com.br), a qualquer momento, que sejam eliminados os seus dados pessoais não anonimizados.

9. DIREITOS DO TITULAR

O titular dos dados pessoais tem direito a obter do Controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I – confirmação da existência de tratamento;
II – acesso aos dados;
III – correção de dados incompletos, inexatos ou desatualizados;
IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade a Lei nº 13.709/18;
V – eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da Lei nº 13.709/18;
VI – informação das entidades públicas e privadas com as quais o Controlador realizou uso compartilhado de dados;
VII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
VIII – revogação do consentimento, quando aplicável nos termos do § 5º do art. 8º da Lei nº 13.709/18.

O Titular de dados pessoais poderá exercer esses direitos entrando em contato com o Controlador pelo e-mail: ouvidoria@safaricapital.com.br.

Os administradores do Controlador (Srs. Elsom Yassuda e Marcelo Cavalheiro) são os Encarregados (*Data Protection Officer* – DPO) para os fins da lei geral de proteção de dados.

10. TÉRMINO DO TRATAMENTO

Esta Política de Privacidade se aplica às circunstâncias acima mencionadas durante todo o período em que o Controlador armazenar os dados pessoais do Titular.

11. ALTERAÇÃO NA POLÍTICA DE PRIVACIDADE

O Controlador se reserva no direito de alterar esta política de privacidade a qualquer momento, mediante publicação da versão atualizada em seu site (www.safaricapital.com.br).

Essa Política de Privacidade entra em vigor em outubro de 2020.

A versão completa deste documento poderá ser consultado no site da instituição por meio do seguinte link: https://safaricapital.com.br/governanca/