Falconi CAPITAL

POLÍTICA DE SEGURANÇA DE INFORMAÇÃO

Índice

OBJETIVO 2
ABRANGÊNCIA 2
TERMOS E DEFINIÇÕES 3
PREMISSAS 4
PROGRAMA DE SEGURANÇA DA INFORMAÇÃO 5
PROPRIEDADE DOS RECURSOS DE TI 8
REGRAS E RESPONSABILIDADES DO USO DE INTERNET 11
USO DE CORREIO ELETRÔNICO PROFISSIONAL 12
MONITORAMENTO E TESTES PERIÓDICOS 16
PLANO DE RESPOSTA 16
POLÍTICA DE PROTEÇÃO A DADOS PESSOAIS 18
VIGÊNCIA E ATUALIZAÇÃO 25

OBJETIVO

Esta Política tem por objetivo contribuir para o aprimoramento da segurança, tanto informacional quanto cibernética da Falconi Capital Ltda. ("Falconi Capital" ou "Gestora"), estabelecendo medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízo para a consecução de suas atividades.

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

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

Qualquer informação sobre a Falconi Capital, ou de qualquer natureza relativa às atividades da empresa e a seus sócios e clientes, obtida em decorrência do desempenho das atividades normais do Colaborador, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pelo Diretor de Risco e Compliance, nos termos estabelecidos no Código de Ética da Gestora.

ABRANGÊNCIA

Os procedimentos aqui estabelecidos se aplicam à Falconi Capital e aos seus Colaboradores, em atendimento aos requisitos do sistema de gestão de compliance.

De forma subsidiária, na ausência de quaisquer medidas indicadas nesta política, a Falconi Capital seguirá as Políticas de Segurança da Informação e Privacidade e Proteção de Dados do Grupo Falconi, naquilo que for aplicável ao seu negócio, bem como os procedimentos, guias*, playbooks* e demais documentos que sucederem e detalharem as referidas políticas.

A efetividade desta Política depende da conscientização de todos os Colaboradores e do esforço constante para que seja feito bom uso das Informações Confidenciais, Dados Pessoais e dos ativos disponibilizados pela Falconi Capital ao Colaborador.

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

TERMOS E DEFINIÇÕES

Acordo de confidencialidade e responsabilidade: Acordos assinados entre duas partes que irão realizar algum tipo de troca ou compartilhamento de informações visando proteger em especial a confidencialidade das informações.

Agentes de tratamento: o controlador e o operador.

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.

Ativos de informação: Qualquer recurso que tenha a capacidade de processar, armazenar ou transmitir informação e a própria informação.

Classificação da informação: Atividade de inventariar e categorizar as informações, definir seu grau de sensibilidade e o grupo de acesso.

Colaboradores: Empregados, estagiários, prestadores de serviço, visitantes e terceiros.

Confidencialidade: Propriedade de que a informação não seja disponibilizada ou divulgada a indivíduos, entidades ou processos não autorizados.

Consentimento: É a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Conta de acesso: Identificação de acesso, pessoal e intransferível. Ela identifica os usuários e define seu perfil de acesso aos recursos de TI.

Controlador: É a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Dados Pessoais: Qualquer informação relacionada a uma pessoa natural identificada ou identificável. Em outras palavras, qualquer informação, independente de formato (físico ou eletrônico), que possa permitir a identificação de uma pessoa natural, ou que, identificada a pessoa, possa ser associada a ela, revelando característica a seu respeito.

Dado Pessoal Sensível: Somente aqueles descritos na Lei como Dados Pessoais Sensíveis, ou seja, o dado pessoal que verse sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Disponibilidade: Propriedade de ser acessível e utilizável sob demanda, por uma entidade autorizada.

Encarregado pelo Tratamento de Dados Pessoais: O Encarregado, ou Data Protection Officer ("DPO"), é a pessoa (natural ou jurídica) indicada pelo agente de tratamento (controlador ou operador) para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). É ao Encarregado que você deve direcionar toda e qualquer requisição acerca do tratamento de seus dados pessoais.

Informação: É um ativo que, como qualquer outro ativo importante, é essencial para os negócios da Falconi Capital e consequentemente necessita ser adequadamente protegida. A informação pode existir de diversas formas. Ela pode ser impressa, escrita em papel, pode ser verbal, gravada, codificada ou ser expressa por meio dos mais diferentes meios e formas de comunicação possíveis, como transmitida pelo correio ou por meios eletrônicos.

Integridade: Propriedade da exatidão e completude da informação. Condição na qual a informação ou os recursos de processamento da informação são protegidos contra modificações não autorizadas.

Segurança da Informação (SI): É a proteção da informação dos vários tipos de ameaças a fim de garantir a continuidade dos negócios e minimizar os riscos associados. Essa proteção é realizada por meio da preservação da confidencialidade, integridade e disponibilidade das informações. A segurança da informação é obtida a partir da implantação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, diretrizes, estruturas organizacionais, treinamento, comunicação e conscientização além de softwares e hardwares específicos.

Titular dos dados: Pessoa natural a quem se referem os dados pessoais que são objeto do tratamento.

Tratamento da informação: Uso adequado da informação de acordo com as diretrizes estabelecidas nos diversos cenários que ocorrem no dia a dia, como armazenamento, transmissão, descarte, impressão etc.

PREMISSAS

Diante da possibilidade de vazamento, alteração, destruição e qualquer outra forma de prejuízo em relação às Informações Confidenciais, que são de extremo valor para a Falconi Capital, à luz do princípio fundamental de confiança que a instituição trabalha para manter junto aos seus cotistas, a Falconi Capital utilizou como linha de estruturação de sua Política, o Guia de Cibersegurança, da ANBIMA, datado de dezembro de 2017. Referido documento é

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

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

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

Ademais, para implementação e monitoramento contínuo da presente Política, a Falconi Capital conta com o suporte de empresa do grupo econômico que integra, à luz do Acordo Operacional firmado entre as partes.

PROGRAMA DE SEGURANÇA DA INFORMAÇÃO

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

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

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

- *Malware* – *softwares* desenvolvidos para corromper computadores e redes:
- Vírus: *software* que causa danos a máquina, rede, *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;
- Acesso pessoal; pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.
- Ataques de DDoS (*distributed denial of services*) e *botnets* - ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos *botnets,* o ataque vem de um grande número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.
- Invasões (*advanced persistent threats*) - ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ainda, além de ataques cibernéticos, a Falconi Capital pode estar sujeita a mal funcionalidades dos sistemas utilizados e a atos ou omissões de seus Colaboradores, que podem acarretar a perda e/ou adulteração de dados e Informações Confidenciais.

Ação 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 Falconi Capital, assim como aquelas que teriam o maior impacto financeiro, operacional e reputacional para Falconi Capital, em caso de incidente de segurança. Deste modo, a Falconi Capital 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 4 (quatro) classes diferentes, quais sejam:

Públicas

Devem ser classificadas como PÚBLICAS, as informações que podem ser divulgadas publicamente e não necessitam de atenção especial quanto à preservação de sigilo. São passíveis de classificação como PÚBLICAS, dados ou informações que podem ser divulgadas para o mercado ou para a comunidade em geral.

Exemplos: Informações divulgadas a investidores e ao mercado, telefones de atendimento ao público, sites institucionais da empresa na Internet e em mídias sociais etc.

Internas

Devem ser classificadas como INTERNAS as informações que devem ser divulgadas a todos os colaboradores da Falconi Capital e/ou para terceiros formalmente comprometidos com a segurança das informações. A informação somente deve ser classificada como INTERNA se for necessário que todos os colaboradores da Falconi Capital tenham conhecimento de tal informação.

Exemplos: Listas de ramais internos, campanhas e comunicações internas, divulgações de metas da Gestora, normas e procedimentos de aplicação geral na Falconi Capital, etc.

Restritas

Devem ser classificadas como RESTRITAS as informações que devem ser divulgadas apenas para algumas pessoas, grupos de trabalho ou áreas da Falconi Capital e que não devem ser divulgadas abertamente a todos os colaboradores da Falconi Capital. A perda destas informações pode gerar impactos em processos, produtos ou serviços específicos da Gestora.

Exemplos: Informações de projetos internos, dados ou informações referentes a produtos, processos e serviços, procedimentos do SGSI, procedimentos operacionais (POP), indicadores de desempenho das áreas, relatórios de auditoria, relatórios específicos das áreas etc.

Confidenciais

Informações que requerem forma de proteção mais robusta contra acesso e compartilhamento não autorizado. Devem ser classificadas como CONFIDENCIAL todas as informações relativas a:

- Informações privadas das pessoas;
- Informações estratégicas de clientes e fornecedores;

- Informações estratégicas da Falconi Capital;
- *Know How* da Falconi Capital;
- Informações que prejudicam a reputação e imagem da Falconi Capital.

São informações cujo perda, roubo, acesso indevido ou não autorizado podem trazer sérios problemas para a reputação, imagem, ações judiciais, gerar passivo trabalhista e prejuízos financeiros diretos com eventual perda de competitividade para a Falconi Capital.

Exemplos: Atas de reuniões estratégicas do Conselho de Administração, contratos com cotistas e fornecedores, informações sobre os projetos com os cotistas, balanço da empresa, informações pessoais e privadas dos colaboradores, informações sobre o método da Falconi Capital, know how relativo a produtos e serviços, feedback dos colaboradores, etc.

A partir da definição acima, a Falconi Capital 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: Públicas, Internas, Restritas, Confidenciais.

PROPRIEDADE DOS RECURSOS DE TI

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

Disponibilização e Uso

Todos os computadores disponibilizados para os Colaboradores da Falconi Capital têm por objetivo o desempenho das atividades na Falconi Capital. 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 equipe de T.I responsável, mediante solicitação de Colaboradores da Gestora, que pressupõe a aprovação do Diretor de Risco e Compliance.

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

- A cada novo Colaborador, o Diretor de Risco e Compliance autorizará 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 equipe de T.I., mediante supervisão e aprovação do Diretor de Risco e Compliance, quando julgar necessário;
- O Diretor de Risco e Compliance autorizará, a retirada ou substituição do computador disponibilizado para o usuário, quando aplicável;
- Cada computador tem o seu usuário gestor, que é responsável por esse equipamento. O controle das máquinas é de responsabilidade da equipe de T.I. responsável, mediante supervisão e aprovação do Diretor de Risco e Compliance, quando aplicável;
- A identificação do usuário é feita através do login e senha, que através do registro de logs utilizado pela Falconi Capital é sua assinatura eletrônica no servidor da Falconi Capital;
- 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;
- Quando aplicável, não será permitida a utilização da mesma senha para projetos e produtos diferentes realizados pela Falconi Capital, não devendo ser criada uma senha única padrão para todos os serviços e áreas em que um mesmo Colaborador atue;
- É permitida apenas 5 tentativas máximas de autenticação de senha, sendo todas malsucedidas, será bloqueado o acesso, o qual apenas poderá ser reestabelecido atravésde solicitação ao Diretor de Risco e *Compliance.*
- As senhas possuem validade de 90 (noventa) 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 sersolicitados pelo Diretor de Risco e Compliance à área responsável.

Softwares

A implantação e configuração de *softwares* da Falconi Capital 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 Diretor de Risco e Compliance, quando necessário;
- É desabilitado ao usuário implantar ou alterar componentes físicos em seus computadores;
- Somente é permitido o uso de equipamentos homologados e devidamente contratados pela Falconi Capital;

- A utilização de equipamentos pessoais por terceiros nas instalações da Falconi Capital e a conexão destes na rede interna à Internet requer autorização 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 do Diretor de Risco e Compliance.

Registros

A Falconi Capital mantém por, no mínimo, 5 anos os *logs* do sistema que utiliza para a realização de suas 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 Falconi Capital, a gestora consegue manter a integridade, autenticidade e audibilidade das informações e sistemas, conforme Resolução CVM n.º 21/2021.

Responsabilidade 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 Falconi Capital.

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 Falconi Capital 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 Falconi Capital.

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);
- 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.

REGRAS E RESPONSABILIDADES DO USO DE INTERNET

O Colaborador é responsável por todo acesso realizado com a sua autenticação. Quando o usuário se comunicar através de recursos de tecnologia da Falconi Capital, este deve sempre resguardar a imagem da Falconi Capital, evitando entrar em sites de fontes não seguras, ou de fontes não conhecidas, salvo quando comunicado e devidamente autorizado pelo Diretor de Risco e Compliance.

O usuário não deve 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;
- 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.

É proibido o uso de serviços de mensagem instantânea (MSN, Skype, etc), através dos computadores da Falconi Capital, exceto em eventuais situações de uso profissional, salvo autorização do Diretor de Risco e Compliance.

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 Falconi Capital.

USO DE CORREIO ELETRÔNICO PROFISSIONAL

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

O endereço eletrônico disponibilizado para o usuário é individual, intransferível e pertence à Falconi Capital. O endereço eletrônico cedido para o usuário deve ser o mesmo durante todo o seu período de vínculo com a Falconi Capital.

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

Endereço Eletrônico de Programas ou 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 Falconi Capital, 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 Falconi Capital.

Acesso à distância ao e-mail

O usuário pode acessar o seu correio eletrônico cedido pela Falconi Capital 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 Falconi Capital.

Responsabilidades e Forma de Uso do 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 Falconi Capital.

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 Falconi Capital, 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 Falconi Capital; e
- Sejam incoerentes com o Código de Ética Corporativa da Falconi Capital.

O Colaborador deve estar ciente que uma mensagem de correio eletrônico da Falconi Capital 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 Falconi Capital.

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.

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.

Armazenamento em Nuvem (*Cloud*)

A Falconi Capital 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.

Fornecedores, prestadores de serviços e parceiros ("Terceiros") podem representar uma fonte significativa de riscos para a Falconi Capital 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.

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, salvo quando estes Terceiros sejam integrantes do grupo econômico do qual a Falconi Capital pertence.

Com isto em mente, a empresa objeto de contratação deverá enviar a Falconi Capital:

1. Documentos que atestem a existência dos respectivos procedimentos de Cibersegurança;
2. Último relatório de teste/auditoria periódica;
3. 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 Falconi Capital.

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 Falconi Capital, 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.

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 no mínimo anual.

Os Testes de Contingência serão realizados anualmente, de modo a permitir que a Falconi Capital 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 Falconi Capital.

Ademais, serão realizados Testes Periódicos de Segurança a Falconi Capital, 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 Falconi Capital, 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 Falconi Capital.

PLANO DE RESPOSTA

Conforme as melhores práticas de mercado, a Falconi Capital 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):

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

Compliance ou Jurídico Contratado:

- 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;
- Em caso de confirmação do incidente de segurança e eventual vazamento de informações confidenciais, elaborar notificação aos clientes afetados informando o ocorrido.

BackOffice:

- Análise de dados perdidos e suas influências frente ao planejamento contábil e aos ativos da Companhia;
- Realizar planejamento de contenção de risco de liquidez frente a possibilidade de resgate de investimentos da Falconi Capital 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 Falconi Capital.

A Falconi Capital 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 Falconi Capital.

POLÍTICA DE PROTEÇÃO A DADOS PESSOAIS

A Falconi Capital 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 Falconi Capital, 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 Falconi Capital.

Importante observar que o escopo da proteção de dados pessoais no âmbito da Falconi Capital 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 Falconi Capital manteve contato para atender alguma demanda relevante e específica. Em ambas as searas, é importante interpretar a atuação da Falconi Capital à luz do Artº 7, II, da Lei 13.709/2018 ("LGPD").

Vale ressaltar que todo o tratamento de dados pessoais feito pela Falconi Capital está pautado nos requisitos do artigo 7º da LGPD, assim como nas premissas do artigo 11 da mesma Lei, quando aplicável.

Princípios Norteadores:

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

- finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- 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;
- 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;
- 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;
- 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;
- 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;
- prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
- 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.

Operações de Tratamento de Dados Pessoais de colaboradores e/ou terceiros

A Falconi Capital possui operações de tratamento de dados pessoais mapeadas para finalidades distintas, mas todas relacionadas ao exercício da sua atividade e aos seus deveres legais e regulatórios, havendo fundamentos legais e legítimos que autorizam e justificam o tratamento, dos quais podemos destacar os seguintes:

- Recrutamento e seleção de colaboradores, consultores, trainees, estagiários e jovens aprendizes;
- Realização de exames admissional, demissional e periódico;
- Recolha pública de dados em rede aberta para fins de investigação e verificação de antecedentes (Background Check), nos casos determinados em lei e/ou regulação atinente à atividade da Falconi Capital.
- Monitoramento do ambiente físico para garantir segurança de toda empresa;
- Oferecimento e Gestão de benefícios obrigatórios e/ou opcionais aos colaboradores;
- Criação e desativação de usuário nos processos de admissão e desligamento de colaboradores;
- Abertura de chamados técnicos para resolução de problemas;
- Gerenciamento de funcionários e o controle de folha de ponto;
- Pagamento de salários, dividendos, bônus e outros pagamentos em geral, incluindo reembolso de custos;
- Compra de passagens aéreas e reservas em hotéis e gestão das viagens corporativas e reembolso de despesas corporativas no desempenho das atribuições dos colaboradores deslocados;
- Acesso à intranet e aos sistemas de apoio para viabilização de tarefas internas dos colaboradores;
- Uso da imagem do colaborador para uso em materiais promocionais da Falconi Capital;
- Promoção de eventos, sorteios ou campanhas educacionais;
- Realização de avaliação de desempenho e avaliação de entrega de resultados;
- Realização de treinamentos para aprimoramento de habilidades dos colaboradores e monitoramento da realização desses treinamentos;
- Pesquisa de clima organizacional e pesquisa termômetro;
- Gestão de caixa e de operações financeiras;
- Atuação em jurídico contencioso e consultivo e postulação judicial em favor da Falconi Capital;
- Atendimento a leis, normas, regulamentos, decisões judiciais ou de autoridades administrativas relacionadas e inerentes ao negócio;
- Apuração de ocorridos por meio do Canal de Denúncias;

- Arquivamento de documentos físicos e eletrônicos por empresa terceirizada especializada;
- Criação de políticas afirmativas e discussão sobre diversidade e inclusão na empresa;
- Compartilhamento de dados pessoais com empresas integrantes do Ecossistema para encontrar soluções para problemas percebidos;
- Geração de *leads* por meio de coleta de dados pessoais em *landing pages* no site da Falconi Capital e gerenciamento desses dados para direcionamento de campanhas de *marketing*;
- Geração de *leads* por meio de coleta de dados pessoais em posts pagos e em perfis de usuários de redes sociais;
- Coletas de *cookies* no site da Falconi Capital para funcionalidades diversas;
- Promoção de eventos, sorteios ou campanhas educacionais;
- Acesso à rede Wi-Fi da Falconi Capital;
- Controle de acesso físico dos visitantes da Falconi Capital;
- Monitoramento do ambiente físico para garantir segurança aos transeuntes da Falconi Capital;

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 Falconi Capital, em relação aos seus dados, a qualquer momento e mediante requerimento expresso o que se segue:

(i) confirmação de existência de tratamento;
(ii) acesso aos dados;
(iii) correção de dados incompletos, inexatos ou desatualizado;
(iv) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei 13.709/2018;
(v) 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;
(vi) 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;
(vii) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

(viii) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e
(ix) revogação do consentimento, nos termos da Lei.

A Falconi Capital disponibiliza canal de comunicação, através do endereço dados@falconicapital.com, ou através do seu Portal de Gestão dos Direitos do Titular, 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 Falconi Capital, os titulares dos dados (pessoas físicas) e a ANPD.

Além disso, qualquer titular poderá gerenciar seus consentimentos, nos casos em que o tratamento dos seus dados se fundamentar somente nesta base legal, através do Centro de Preferências da Falconi Capital, sem a necessidade de abrir uma requisição.

Período de Armazenamento dos Dados Pessoais

Os dados pessoais serão armazenados pela Falconi Capital 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. Os períodos de armazenamento e retenção de dados que ultrapassam o prazo mínimo definido retro estão detalhados na Política de Retenção de Exclusão de Dados Pessoais da Falconi Capital.

Cooperação com Autoridades

A divulgação de dados pessoais para o cumprimento de lei, determinação judicial, regulatória ou de órgão competente ao qual a Falconi Capital 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 Falconi Capital, serão notificados sobre tal divulgação, para que tomem as medidas apropriadas.

Adicionalmente, a Falconi Capital 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 apresentadas pelo Encarregado pelo Tratamento de Dados Pessoais para deliberação no Comitê de Gestão de Riscos e de Compliance.

Obrigação de Reporte

Os Colaboradores estão obrigados a comunicar imediatamente ao Encarregado pelo Tratamento de Dados Pessoais, através do e-mail dados@falconicapital.com, sobre toda e qualquer suspeita ou indício de evento que possa ter comprometido os dados pessoais de posse da Falconi Capital 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, assim como aquelas operações que podem gerar riscos às liberdades civis e aos direitos fundamentais do titular, em especial aquelas que tratam dados pessoais sensíveis e aquelas fundamentadas no legítimo interesse da Falconi Capital e/ou de terceiros, serão registrados no Relatório de Impacto à Proteção de Dados Pessoais, nos termos da LGPD e regulamentações dos órgãos competentes.

Transferência Internacional

A Falconi Capital admite a transferência internacional de dados pessoais para países estrangeiros apenas nos seguintes casos:

(i) Para países ou organismos internacionais que a ANPD considere que proporcionem grau de proteção de dados pessoais adequado ao previsto na LGPD ou quando a ANPD autorizar a transferência.
(ii) No momento da elaboração desta versão da Política inexistem países considerados como adequados pela ANPD. Sendo assim, enquanto não divulgação de tais países, a Falconi Capital admite a transferência internacional para países classificados como adequados aos critérios da GDPR pelo Comitê Europeu de Proteção de Dados (CEPD), por meio de uma Decisão de Adequação;
(iii) Quando o agente de tratamento oferecer e comprovar à Falconi Capital garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

- cláusulas contratuais específicas para determinada transferência;
- cláusulas-padrão contratuais definidas pela ANPD ou pelo Comitê Europeu de Proteção de Dados (CEPD);
- normas corporativas globais aprovadas pela ANPD ou pelo Comitê Europeu de Proteção de Dados (CEPD);
- elos, certificados e códigos de conduta regularmente emitidos e reconhecidos e aprovados pela ANPD ou pelo Comitê Europeu de Proteção de Dados (CEPD);

(iv) Quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades.

Treinamento

A Falconi Capital treinará seus Colaboradores sobre a proteção de dados pessoais e de dados sigilosos, de acordo com a seu Plano Anual de Treinamentos, aprovado pela alta liderança da empresa.

Em complemento, a Falconi Capital oferecerá treinamentos periódicos e específicos sobre privacidade e proteção de dados nas modalidades de cursos *online*, *workshops*, reuniões internas, conversas regulares, palestras, dentre outras iniciativas, cujo objetivo será construir uma cultura corporativa referente ao tema, bem como para que todos os stakeholders tenham conhecimento sobre essa política e demais normas internas da Falconi Capital referentes à privacidade, proteção de dados e segurança da informação.

A depender do modo aprovado pela alta liderança, será obrigatória a participação nos treinamentos dos colaboradores da Falconi Capital cujos *job descriptions* estabeleçam o tratamento regular de dados pessoais.

Em tais casos, a base legal para o tratamento dos dados pessoais é o legítimo interesse do Controlador, sendo de total interesse da Falconi Capital possuir colaboradores cada vez mais atualizados e afiados com sua cultura e suas expectativas, cumprindo o propósito de impactar positivamente a sociedade.

VIGÊNCIA E ATUALIZAÇÃO

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

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

CONTROLE DE VERSÕES	DATA	MODIFICADO POR	DESCRIÇÃO DA MUDANÇA
1	Fevereiro/2022	RRZ Consultoria	Versão inicial
2	Maio/2023	Comitê de Risco & Compliance	Revisão Periódica