POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Versa Gestora de Recursos Ltda.

ÍNDICE

CONTROLE DE VERSÕES

Versão	Revisão	Revisor
1.0	Setembro/2017	Versão Inicial
1.1	Outubro/2021	**Risco e Compliance**
1.2	Junho/2022	**Risco e Compliance**
1.2	Fevereiro/2024	**Risco e Compliance**

INTRODUÇÃO

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

As medidas de segurança e procedimentos descritas nesta política têm por finalidade minimizar as ameaças ao patrimônio, à imagem e aos negócios da empresa. Sendo assim, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Versa, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

Qualquer informação sobre a Versa, 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 *Compliance*.

O disposto nesta Política deve ser observado durante a vigência do relacionamento profissional do Colaborador com a Versa e após seu término.

CLASSIFICAÇÃO DA INFORMAÇÃO

Para fins desta Política, considera-se como informação:

- Todo tipo de informação escrita, verbal ou apresentada de modo tangível ou intangível, podendo incluir: 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 investidores, dos clubes, fundos de investimento e carteiras geridas pela Gestora, operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento e carteiras geridas pela Gestora, estruturas, planos de ação, relação de investidores, 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 investidores, independente destas informações estarem contidas em discos, disquetes, pen-drives, fitas, outros tipos de mídia ou em documentos físicos
- 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, investidores, fornecedores e prestadores de serviços em geral.

Visando garantir a proteção necessária, os documentos de posse da gestora devem ser classificados de acordo com sua confidencialidade, nos seguintes níveis: Pública, Interna e Confidencial.

Tipo da informação	Descrição
Pública	A informação deve ser classificada como pública quando ela puder ser divulgada a todos, isto é, funcionários, terceirizados, clientes, fornecedores e público em geral, sem que isso provoque impactos no negócio.
Interna	A informação deve ser classificada como interna quando não for desejável que ela se torne conhecida por pessoas de fora da organização. Contudo, caso haja vazamento e ela se torne de conhecimento público, é característica da informação classificada como interna a impossibilidade da ocorrência de um grande prejuízo à organização.
Confidencial	A informação deve ser classificada como confidencial quando sua exposição fora do ambiente da organização possa acarretar em perdas financeiras, de imagem, de competitividade etc.

Como regra geral, deve ser sempre atribuída a classificação mais restritiva ao documento que contiver as informações de diferentes graus de confidencialidade.

RESPONSABILIDADES

A Política de Segurança da Informação, 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 Versa, ou que acesse informações a ela pertencentes.

Todo colaborador da Versa tem a responsabilidade de implementar e reforçar os procedimentos utilizados a fim de proteger a confidencialidade das informações

Seguindo o disposto no Código de Administração de Recursos de Terceiros da ANBIMA, todos os colaboradores da Versa e/ou terceiros contratados devem assinar o termo de confidencialidade sobre as informações que lhe foram confiadas em virtude do exercício de suas atividades profissionais.

A Versa indica como responsável dentro da instituição para tratar e responder questões de segurança cibernética o Diretor de *Compliance*.

SEGURANÇA DA INFORMAÇÃO

Controle de acesso a dados físicos

Embora quase a totalidade de arquivos estejam em formato digital, arquivos físicos, papéis e documentos podem ser mantidos dentro do escritório da Gestora, cujo acesso é controlado. O acesso ao escritório requer senha e/ou biometria concedida exclusivamente para Colaboradores autorizados.

É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis da Versa e circulem em ambientes externos à empresa com os mesmos, sem prévia autorização do Diretor de *Compliance*. Isso porque tais arquivos contêm informações que são consideradas informações confidenciais.

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 Versa. 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 Versa.

Controle de acesso a dados eletrônicos

Os computadores e pastas digitais são protegidas por login e senha individualizados, e apenas as pessoas previamente autorizadas podem acessá-los. O acesso às informações é fornecido aos Colaboradores cuja necessidade é justificada.

A definição de senhas de acesso a dispositivos corporativos, sistemas e redes devem ter um nível mínimo de complexidade adotando uso de maiúsculas/minúsculas e caracteres numéricos. As senhas devem ser trocadas periodicamente e devem ser segregadas entre serviços (não deve ser utilizada uma mesma senha para acessar diversos sistemas). Além disso, sempre que houver a possibilidade, deve-se adotar a autenticação de múltiplos fatores.

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, é proibida a conexão de equipamentos na rede da Versa que não estejam previamente autorizados, para tanto os Colaboradores devem se abster de utilizar pen-drives, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Versa.

Programas instalados nos computadores, principalmente via internet (downloads), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia dos sócios. Não é permitida a instalação de nenhum software ilegal ou que possuam direitos autorais protegidos. Softwares e sistemas operacionais devem sempre ser atualizados, de forma que sejam mantidos sempre com a maior proteção possível.

Por fim, convém ressaltar que a Versa conta com sistemas com sistemas contratados para arquivamento, firewall, antivírus, backup, linhas telefônicas com gravação e linha metálica de contingência.

Monitoramento

Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

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 Versa.

Todo conteúdo que está na rede pode ser acessado pelos sócios ou pelo Diretor de *Compliance* caso haja necessidade, inclusive e-mails. Arquivos pessoais salvos em cada computador poderão ser acessados caso seja necessário. 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 a determinações judiciais ou administrativas.

Armazenamento e descarte de informação

Seguindo a classificação de informações segundo a confidencialidade, devem ser observadas os seguintes procedimentos para armazenamento e descarte de documentos físicos ou digitais.

Informação Física	**Armazenamento**	**Descarte**
Pública	Pode ser armazenada em área sem restrição de acesso	Forma simples, sem uso de recursos e procedimentos para descarte
Interna	Armazenar em áreas de acesso seguro (ex.: dentro do escritório)	Analisar as informações e, se necessário, descartar junto às informações confidenciais.
Confidencial	Armazenar em local seguro com restrição de acesso. (ex.: trancado em uma gaveta no escritório)	Utilizar procedimento ou ferramenta que destrua a informação por completo.

Informação Digital	Armazenamento	Descarte
Pública	Backups regulares para garantir a integridade e disponibilidade	Forma simples, sem uso de recursos e procedimentos para descarte
Interna	Armazenar em áreas de acesso restrito (com controle de acesso)	Analisar as informações e, se necessário, descartar junto às informações confidenciais.
Confidencial	Armazenar em áreas de acesso restrito (com controle de acesso) e com verificação de senha.	Utilizar procedimento ou ferramenta que destrua a informação por completo.

Backup **e redundância**

A empresa utiliza os serviços do Google para armazenamento de arquivos, sendo que todos os arquivos da empresa são salvos no serviço de armazenamento em nuvem do Google. Adicionalmente, é feito o backup dos mesmos arquivos para um servidor dedicado três vezes ao dia.

Para o armazenamento de dados, a empresa utiliza serviço da Amazon de armazenamento em nuvem.

Os serviços de armazenamento de dados em nuvem têm padrão internacional de conformidade, contam com proteção criptográfica, controle de nível de acesso lógico por usuário, backup e restauração de arquivos e são armazenados em data centers seguros. Além disso, os serviços em nuvem contam com sistema de proteção contra práticas fraudulentas e/ou suspeitas, de forma que o administrador de rede/servidor é notificado e pode agir de modo a mitigar as vulnerabilidades.

SEGURANÇA CIBERNÉTICA

Risk Assessment

A gestora deverá identificar e avaliar os principais riscos cibernéticos as quais está exposta. Como definido no Guia Anbima de Cibernética, os tipos mais comuns são:

- Malwares
- Engenharia Social
- Pharming
- Phishing Scam
- Vishing
- Smishing
- Acesso Pessoal
- Ataques DDoS e botnets
- invasões.

Devido à natureza da atividade exercida pela gestora, o *Risk Assessment* inicial identifica como principais riscos o (I) vazamento de informações e o (II) comprometimento da integridade e/ou disponibilidade da informação.

Para o primeiro caso(I), existe um conjunto de procedimentos internos pré-definidos na eventualidade de uma ocorrência, que estão descritos na seção de plano de resposta a incidentes desta política.

No segundo caso (II), para dados eletrônicos, a segurança da informação foi considerada na própria contratação dos serviços de armazenamento de arquivos e dados, que se deram por empresas de renome e com serviço que possibilita a restauração e backup dos mesmos. No caso de dados físicos, esta política descreve os controles de acesso e as ações permitidas pelos colaboradores, de forma a mitigar a ocorrência. E, no caso de indisponibilidade algum serviço ou de acesso à sede, a política de continuidade de negócios descreve as diretrizes principais dos procedimentos a serem utilizados.

Todo colaborador que identificar riscos não identificados na política, que possam afetar a segurança de informações detidas pela Versa ou riscos nos processos de segurança de informação da gestora, deve informar a área de *Compliance*, para que sejam tomadas as providências cabíveis.

Proteção e Prevenção

As ações de proteção e prevenção estão descritas na seção de Segurança da Informação desta Política.

PLANO DE RESPOSTA A INCIDENTES

Em caso de incidente de segurança, a área de *Compliance* deve ser notificada imediatamente, e em conjunto com a área de Operações, deve realizar uma análise completa e levantamento dos sistemas e informações afetadas, elaborando plano de resposta a incidentes de acordo com as etapas a seguir:

Etapa	**Descrição**
Identificação	Os incidentes devem ser identificados conforme sua categoria, êxito de ataque, sistemas afetados, evidências etc. Cada incidente deve ser classificado conforme sua criticidade e deve ter sua causa identificada e documentada.
Contenção	A área responsável pela segurança da informação, deve determinar o plano para conter os danos, corrigi-los e erradicar a causa raiz.
Controle	Após a etapa de contenção, devem ser realizados os devidos testes para garantir que o incidente foi controlado.
Documentação	O incidente só deve ser dado como encerrado após a documentação com sua identificação, plano de ação, resultados e tudo o que foi realizado em sua contenção.

Em todas as etapas devem ser observadas os procedimentos e diretrizes de controles internos de privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética.

O grupo de trabalho responsável pelo plano de resposta e por sua execução deve se reportar ao Comitê de *Compliance.*

Plano de resposta a vazamento de dados

Na eventualidade de ocorrer um vazamento de quaisquer informações confidenciais, seja de natureza voluntária ou involuntária, a área de *Compliance* é a responsável por tomar ciência, identificar potenciais riscos e executar o plano de resposta a incidentes.

A partir do conhecimento da informação vazada, deverá ser identificado o tipo de vazamento, analisando se há referência aos fundos de investimento ou se o vazamento é relativo a dados pessoais de colaborares, investidores, fornecedores, terceiros contratados ou da própria Gestora.

No caso de vazamento de informações relativas aos fundos de investimento geridos, caso necessário, deverá ser publicado comunicado ou fato relevante, nos termos da regulamentação vigente, a fim de garantir a ampla disseminação e tratamento equânime da informação. Este procedimento procura garantir que nenhuma pessoa seja beneficiada com o uso da informação vazada.

No caso de outros vazamentos, conforme o caso, deverá ser feito todo o possível para cessar a disseminação da informação e conter seus impactos. Para tanto, dentre outras medidas, poderão ser autorizadas: (i) contratação de empresa especializada em consultoria para proteção/recuperação de dados; (ii) contratação de advogados especializados na matéria.

TREINAMENTO

A Versa promove e dissemina a cultura da segurança da informação, entendendo ser essencial que seus Colaboradores estejam cientes e consonantes dos procedimentos e diretrizes adotadas nesta Política.

TESTES PERIÓDICOS

Como forma de garantir e verificar o funcionamento dos sistemas de segurança, a Versa se reserva ao direito de:

- Implantar softwares e sistemas que podem monitorar e gravar todos os usos de Internet através da rede e das estações de trabalho da empresa, respeitado o direito à intimidade e ao sigilo das comunicações, nos termos do art. 5º, X e XII, da Constituição Federal;
- Inspecionar qualquer arquivo armazenado na rede, estejam no disco local da estação ou nas áreas privadas da rede, visando assegurar o rígido cumprimento desta política;
- Efetuar verificações e auditoria pela equipe de Infra/Segurança nos sistemas, estações e rede sem aviso prévio;

Periodicamente, a Versa poderá realizar testes dos seus sistemas de segurança de informações, bem como de todos os preceitos contidos na presente política, incluindo, mas não se limitando apenas aos procedimentos de descarte de informações pelos Colaboradores, individualização dos usuários, dentre outros.

No caso de detecção de uso em desconformidade com o estabelecido no documento, poderá ser realizado o bloqueio de acesso ou cancelamento do usuário.

Todos os resultados desses testes, bem como os procedimentos para saneamento de eventuais problemas deverão estar descritos no Relatório Anual de Conformidade.

VIGÊNCIA E ATUALIZAÇÃO

Esta política será revisada periodicamente, 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.