



# **VERSA**

## **GESTÃO DE RECURSOS**

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

**Versa Gestora de Recursos Ltda.**

Janeiro/2018

## ÍNDICE

APRESENTAÇÃO .....	3
OBJETIVOS.....	3
SEGURANÇA DE INFORMAÇÕES .....	3
TREINAMENTO DE SEGURANÇA DAS INFORMAÇÕES .....	5
RELATÓRIO DE TESTES DE SEGURANÇA DAS INFORMAÇÕES .....	5
VIGÊNCIA E ATUALIZAÇÃO.....	5

## **APRESENTAÇÃO**

A Política de Segurança da Informação da Versa Gestora de Recursos Ltda. (“Versa”), 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 e qualquer usuário de recursos computadorizados da nossa instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

## **OBJETIVOS**

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.

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*.

## **SEGURANÇA DE INFORMAÇÕES**

As medidas de segurança da informação utilizadas pela Versa 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 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.

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, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Versa.

É proibida a conexão de equipamentos na rede da Versa que não estejam previamente autorizados.

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.

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.

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.

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.

### **TREINAMENTO DE SEGURANÇA DAS INFORMAÇÕES**

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

### **RELATÓRIO DE TESTES DE SEGURANÇA DAS INFORMAÇÕES**

Anualmente, a Versa realizará 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.

Todos os resultados desses testes, bem como os procedimentos para saneamento de eventuais problemas serão descritos no Relatório Anual de Controles Internos da Versa.

### **VIGÊNCIA E ATUALIZAÇÃO**

Esta política será revisada anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.