VRMLOG

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação é responsável por orientar e direcionar os padrões de segurança dos dados, adequando-se aos requisitos de negócios e às leis regulamentadoras.

O seu principal objetivo é atender aos três princípios da Segurança da Informação, conhecidos como CID, sigla para:

Confidencialidade: garantia de que as informações serão acessadas somente pelas pessoas autorizadas, e por quem de fato precisa do acesso.

Integridade: garantia de que a informação é a mesma desde o momento que foi gerada até o seu descarte, ou seja, garantia de que a informação seja confiável, íntegra e verdadeira, e que não tenha sofrido nenhum tipo de manipulação.

Disponibilidade: garantia de que a informação estará plenamente acessível sempre que a sua utilização for necessária.

01 APRESENTAÇÃO, OBJETIVO E ABRANGÊNCIA

Esta Política é fruto do compromisso da VRM LOG na preservação do sigilo de todos os dados, informações, documentos e materiais de qualquer natureza e espécie, que forem disponibilizados ou obtidos no exercício de suas atividades.

Esta Política foi elaborada com o fim de garantir o alinhamento estratégico às atuais normas que regulam as atividades da VRM LOG e às melhores práticas de mercado.

O respeito aos preceitos desta Política e dos demais documentos de integridade da empresa deve ser difundido, assimilado e praticado no dia a dia de todos durante a execução das atividades profissionais, sendo imprescindível que todos colaborem com a estrita observância das regras aqui contidas e se comprometam a comunicar qualquer violação de forma direta aos seus superiores hierárquicos ou pelos canais de comunicação disponibilizados pela empresa.

As diretrizes desta política vinculam e obrigam os colaboradores, diretores, sócios, prestadores de serviços, consultores, parceiros de negócios, fornecedores e todos aqueles que atuem em nome da empresa e/ou em conjunto com ela.

02 DEFINIÇÕES

COLABORADORES E TERCEIROS

Todos os empregados, diretores, sócios, prestadores de serviços, consultores, parceiros de negócios, fornecedores e todos aqueles que atuem em nome da empresa e/ou em conjunto com ela.

INFORMAÇÃO CONFIDENCIAL

Toda informação escrita, computadorizada, oral ou visual, referente à VRM LOG ou a terceiros, recebida ou obtida pelas partes abrangidas pela presente Política, que não são abertas ao público, ou ao mercado em que atua. São consideradas informações confidenciais: critérios de negociação com clientes, precificação, investidores, órgãos governamentais, parceiros, prestadores de serviço, consultores e assessores, e demais informações de caráter comercial, intelectual ou industrial.

A título ilustrativo, informações comerciais incluem:

- Qualquer informação relacionada às atividades da VRM LOG, assim como as informações e dados, sejam eles provisórios ou definitivos, de natureza técnica, comercial, financeira, jurídica, estratégica, ou outra, inclusive, e sem limitação, segredos comerciais, rol e dados de clientes, interessados ou parceiros, dados negociais, know-how, sistema de trabalho, sistemas de informação, planos comerciais, preparação e participação em concorrências públicas ou privadas, ou qualquer outra informação financeira ou econômica, contabilidade, marketing, vendas e procedimentos judiciais, arbitrais ou administrativos, ajuizados ou não, conflitos potenciais ou efetivos;

- Projetos de qualquer espécie, incluindo mas não se limitando a inovação, desenvolvimento de novos negócios, negociações com terceiros.

Caso uma informação confidencial seja incorporada ou refletida em documentos, tanto separadamente ou conjuntamente gerados pela VRM LOG ou a serviço desta, estes documentos deverão ser considerados também como informação comercial.
Dono da informação é o proprietário do dado/informação, ou o seu legítimo possuidor.

HARDWARE

É a parte física do computador, ou seja, o conjunto de aparatos eletrônicos, peças e equipamentos que fazem o computador funcionar.

LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

Lei nº 13.709/2018, que dispõe sobre a privacidade e o uso/tratamento de dados pessoais. Tem como foco a criação de um cenário de segurança jurídica, com a padronização de regulamentos e práticas para promover a proteção aos dados pessoais de todo cidadão que esteja no Brasil, de acordo com os parâmetros internacionais existentes.

RECURSOS DE TI

São recursos associados à aquisição, manutenção ou substituição da infraestrutura, assim como às possibilidades de terceirização dentro do Departamento de TI.

SEGURANÇA DA INFORMAÇÃO

Proteção do conjunto de informações de valor relevante para a VRM LOG, para garantir a confidencialidade, integridade e disponibilidade.

SERVIDOR

Servidor de computação é um computador com um hardware especifico, e sistemas operacionais próprios para entregar serviços para as demais máquinas tanto em rede locais como na internet.

SISTEMAS EMPRESARIAIS – ERP

Sistemas de informação que interligam todos os dados e processos de uma organização.

SOFTWARE

Conjunto de componentes lógicos de um computador ou sistema de processamento de dados; programa, rotina ou conjunto de instruções que controlam o funcionamento de um computador.

TECNOLOGIA DA INFORMAÇÃO - TI

Departamento da empresa que cuida da gestão dos recursos de Tecnologia da Informação.

03 DIRETRIZES

A VRM LOG se orgulha da imagem que vem construindo ao longo do tempo, e que decorre da atuação séria e íntegra que compõe seu DNA empresarial. Por isso, não tolera práticas capazes de atingir ou macular a sua boa fama comercial.

Toda informação produzida e/ou recebida por colaboradores ou terceiros pertence à VRM LOG.

Todos os contratos firmados pela VRM LOG deverão conter cláusula de confidencialidade como condição imprescindível para a concessão do acesso aos ativos de informação disponibilizados pela empresa.

Qualquer incidente que possa afetar a segurança das informações da VRM LOG deverá se comunicado ao Departamento de TI, para as devidas providências. O Departamento de TI é responsável pela guarda das informações, assim como pela adoção de medidas preventivas, detectivas e corretivas com relação a temas relacionados à Segurança da informação. Cabe ainda ao Departamento de TI manter o plano de contingenciamento e continuidade dos principais sistemas, softwares e hardwares, visando reduzir os riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação da VRM LOG.

O site da empresa está hospedado em Servidor em Cloud da Kinghost (https://king.host/), cabendo à empresa terceirizada, devidamente contratada para este fim, geri-lo de acordo com as regras e princípios estabelecidos nas Políticas da empresa.

A VRM LOG mantém, no mesmo Cloud, Servidor que fornece aos seus colaboradores conta de e-mail corporativo, que deverá ser utilizada única e exclusivamente para as atividades diretamente relacionadas ao trabalho. Os colaboradores estão cientes de que o e-mail corporativo não poderá ser acessado em dispositivos que não os disponibilizados pela empresa, e de que os conteúdos nele transacionados são de propriedade da VRM LOG, que poderá, a qualquer tempo, ter livre e amplo acesso, sem que isso configure violação ao direito de privacidade.

Os arquivos relacionados à operação empresarial devem ser obrigatoriamente salvos no Servidor, nunca sendo mantidos apenas nas estações de trabalho.

Os colaboradores devem se atentar aos e-mails com remetentes desconhecidos ou suspeitos, não devendo abrir quaisquer arquivos anexos ou clicar em links fornecidos. Tais situações devem ser comunicadas ao Departamento de TI.

Os equipamentos, tecnologias e serviços fornecidos para o acesso à internet são de propriedade da VRM LOG, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação de trabalho ou em áreas privadas da rede, visando assegurar o cumprimento desta Política.

Nos equipamentos fornecidos pela empresa só estão autorizados os downloads (baixa e/ou instalação) de programas ligados diretamente ao trabalho, devendo o colaborador providenciar o que for necessário para a regularização da licença e/ou o registro desses programas, desde que previamente autorizados pelo Departamento de TI. O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado será excluído pelo Departamento de TI, sem prévio aviso.

A VRM LOG faz uso do sistema TOTVS - WINTHOR, cuja integridade e manutenção são de responsabilidade do Departamento de TI. Faz uso, ainda, de mecanismos disponíveis no mercado para garantir a segurança de seu servidor e de suas informações, mantendo procedimentos e padrões de backup de suas informações gerenciados pelo Departamento de TI.

A VRM LOG trata os dados pessoais de colaboradores e parceiros por meio de seu Departamento de Recursos Humanos, atendendo a todas as determinações da Lei Geral de Proteção de Dados – LGPD, desde o início dos processos de recrutamento e seleção, e durante toda a vigência dos contratos de trabalho, até o desligamento dos colaboradores.

04 POLÍTICA DE CONSEQUÊNCIAS

A VRM LOG não tolerará violações à Política de Segurança da Informação, de forma que qualquer violação será tratada como assunto de extrema gravidade.

Sem prejuízo das sanções legais que possam ser aplicadas, o descumprimento de normas e regras poderá ensejar a aplicação de medidas disciplinares, dentre elas:

- Orientação
- Advertência verbal
- Advertência por escrito
- Suspensão
- Demissão sem justa causa
- Demissão por justa causa

Comunicar o não atendimento das regras de integridade é um dever de todos. Caso presencie ou tome conhecimento da prática de ato em desacordo com as regras desta política, utilize o canal de comunicação através do e-mail compliance@vrmlog.com.br ou https://bcompliance.com.br/empresas/68757817c152b4f1d7c0de99.

As denúncias recebidas serão analisadas e investigadas, sendo garantido ao denunciante, além do direito ao anonimato, a devida proteção contra atos de retaliação.

Elaborado por:
Departamento Jurídico e Compliance

Revisado por:
Departamento de Tecnologia da Informação - TI

Aprovado por:
Diretoria Executiva

Versão: 04
Data de Publicação: 07/2025