SAMESIDE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

FICHA DE CONTROLE

Título	Política de Segurança da Informação
Data	06/06/2022
Versão	1.2
Setor	Compliance, Risco e PLDFT
Responsável	Carlos Schuch
Status	Aprovado
Revisão	Marcos Fritzen
	Guilherme Fração

HISTÓRICO DE VERSÕES

Versão	Alteração	Responsável	Data
1.0	-	Carlos Eduardo El Halal Schuch	31/08/2018
1.1	Formatação	Carlos Eduardo El Halal Schuch	23/11/2021
1.2	Revisão	Carlos Eduardo El Halal Schuch	06/06/2022

SUMÁRIO

1. INTRODUÇÃO E OBJETIVO

Esta Política foi elaborada pela SAMESIDE CONSULTORIA E GESTÃO LTDA (“SameSide”) e tem por objetivo descrever as diretrizes e orientações de segurança da informação e de uso adequado de recursos tecnológicos.

2. VIGÊNCIA E PERIODICIDADE DE REVISÃO

Esta política não tem período de vigência e deve ser atualizada conforme a necessidade e o critério do diretor de “Risco, Compliance e PLDFT”.

3. DIRETRIZES

A informação pode estar presente em diversas formas como, por exemplo, sistemas de informação, diretórios de rede, bancos de dados, mídia impressa ou eletrônica, dispositivos móveis e, até mesmo, por meio da comunicação oral.

Toda informação é um ativo de valor, devendo ser adequadamente utilizada e protegida, conforme a legislação vigente e os procedimentos internos da SameSide.

Toda informação e recurso tecnológico devem ser utilizados com o objetivo de apoiar e suportar o desempenho das atividades da SameSide. Sua utilização deve atender às políticas e procedimentos de segurança da informação.

O uso dos ativos e recursos tecnológicos, inclusive sistemas de informação e serviço de e-mail da SameSide, pode ser monitorado e os registros assim obtidos poderão ser utilizados para avaliação de sua conformidade de uso com as atividades corporativas, podendo servir de evidência para a aplicação de medidas disciplinares, processos administrativos ou legais. As informações geradas e recebidas devem atender às necessidades:

- Disponibilidade: visa a garantir que todas as pessoas autorizadas obtenham acesso à informação e aos ativos correspondentes sempre que necessário;
- Integridade: visa a garantir que a informação esteja sempre completa e íntegra e que não tenha sido modificada ou destruída de maneira indevida (não autorizada ou acidental) durante o seu ciclo de vida;
- Confidencialidade: visa a garantir que a informação seja acessível somente pelas pessoas autorizadas e pelo período necessário;
- Autenticidade: visa a garantir a verificação da identidade dos usuários e à certeza de que a informação provém da origem anunciada;

4. RESPONSABILIDADES

A SameSide e seus colaboradores devem zelar pela manutenção da segurança das informações, aderindo aos cuidados na manutenção das mesas limpas e no tratamento das informações, independente da forma ou meio utilizado, inclusive oralmente. A utilização de dispositivos móveis (smartphones, tablets, etc.) para acessar informações internas é permitida.

O uso destes dispositivos móveis é restrito ao acesso de e-mails e aplicações que sejam formalmente autorizadas, nos termos dos procedimentos de controle vigentes. A eventual utilização para fins profissionais de serviços de mensagem instantânea em smartphones pessoais (WhatsApp, Telegram, Messengers, etc.) deve observar o mesmo zelo e cuidado com a segurança da informação exigidos por esta política e pela relação de fidúcia existente entre as partes.

Ao utilizar recursos pessoais para fins profissionais, o colaborador, caso solicitado, se coloca à disposição da SameSide para cooperar e fornecer informações que eventualmente sejam necessárias para a defesa e preservação dos interesses da SameSide e dos seus clientes.

5. SEGURANÇA DA INFORMAÇÃO CONFIDENCIAL

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

Qualquer informação sobre a SameSide, ou de qualquer natureza relativa às atividades da SameSide, aos seus sócios e clientes, obtida em decorrência do desempenho das atividades normais do colaborador na SameSide, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado por escrito pelo diretor de “Compliance, Riscos e PLDFT”.

É terminantemente proibido que os colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da SameSide e circulem em ambientes externos à SameSide com estes arquivos, uma vez que 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 SameSide e de seus clientes. 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 imediatamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno da SameSide.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Todos os arquivos digitalizados em pastas temporárias serão apagados periodicamente, de

modo que nenhum arquivo deverá ali permanecer. A desobediência a esta regra será considerada uma infração, sendo tratada de maneira análoga à daquele que esquece material na área de impressão.

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.

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

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

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

Em nenhuma hipótese um colaborador pode emitir opinião por e-mail em nome da SameSide, ou utilizar material, marca e logotipos da SameSide para assuntos não corporativos ou após o rompimento do seu vínculo com este, salvo se expressamente autorizado para tanto.

O diretor de “Compliance, Riscos e PLDFT” também monitorará e, será avisado por e- mail em caso de tentativa de acesso aos diretórios e logins virtuais no servidor protegidos por senha. O diretor de “Compliance, Riscos e PLDFT” elucidará as circunstâncias da ocorrência deste fato e aplicará as devidas sanções.

Programas instalados nos computadores, principalmente via internet (downloads), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia do responsável pela área de informática na SameSide. Não é permitida a instalação de nenhum software ilegal ou que possua direitos autorais protegidos. A instalação de novos softwares, com a respectiva licença, deve também ser comunicada previamente ao responsável pela informática. Este deverá aprovar ou vetar a instalação e utilização dos softwares dos colaboradores para aspectos profissionais e pessoais.

A SameSide se reserva no direito de gravar qualquer ligação telefônica e/ou qualquer comunicação dos seus colaboradores realizada ou recebida por meio das linhas telefônicas ou qualquer outro meio disponibilizado pela SameSide para a atividade profissional de cada colaborador. O diretor de “Compliance, Riscos e PLDFT” é encarregado de, a seu critério, monitorar, por amostragem, as ligações e demais comunicações realizadas pelos colaboradores. Qualquer informação suspeita encontrada será esclarecida imediatamente pelo diretor de “Compliance, Riscos e PLDFT”.

Todas as informações da SameSide são armazenadas em servidor Dell PowerEdge 330, com 2 HD de 1 TB. Nesse servidor, as informações são segregadas por área e transformadas em pacotes criptografados, sendo armazenadas com backup e replicada no OneDrive da Microsoft.

Em caso de divulgação indevida de qualquer informação confidencial, o diretor de “Compliance, Riscos e PLDFT” irá apurar o responsável por tal divulgação, sendo certo que poderá verificar no servidor quem teve acesso ao referido documento por meio do acesso individualizado de cada colaborador.

6. REGRAS APLICÁVEIS AOS COLABORADORES

Os recursos de TI disponibilizados para os usuários têm como objetivo a realização de suas atividades profissionais na SameSide. É de responsabilidade de cada usuário assegurar a proteção do recurso computacional, a integridade do equipamento e a confidencialidade da informação nele contida. O usuário não deve alterar as configurações dos equipamentos recebidos.

A utilização de armazenamento em nuvem (cloud) é permitida somente para uso corporativo por meio do parceiro credenciado informado no procedimento interno da SameSide. É vedada a utilização de serviços de nuvem (cloud) de parceiros não-homologados e de serviços de nuvem (cloud) para fins pessoais.

É vedada a instalação de qualquer software/plug-in diretamente pelos colaboradores. A solicitação de instalação deve ser feita exclusivamente pelo canal de TI.

Os colaboradores têm o dever de relatar prontamente à área de TI qualquer fato ou ameaça à segurança dos ativos e recursos tecnológicos da SameSide, tais como quebra da segurança, fragilidade, mau funcionamento, vírus, suspeita de intercepção de mensagens eletrônicas, de acesso indevido e desnecessário a diretórios de rede.