POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

digiteam
LEAD THE WAY

SUMÁRIO

FOLHA DE CONTROLE

Título do documento	Política de Segurança da Informação
Número da versão	1.0/2024
Status	Aprovado
Data da Aprovação	31/01/2024
Área responsável pela elaboração	Equipe de tecnologia com auxílio de jurídico terceirizado
Área de aplicação	Brasil
Classificação da Publicidade	Público interno e externo
Controlador Responsável	DIGITEAM TECNOLOGIA LTDA (DIGITEAM)
CNPJ	07.821.585/0001-50

1. OBJETIVO

A presente **Política de Segurança da Informação ("Política" ou "PSI")** tem como objetivo estabelecer e manter a estrutura destinada à segurança das informações de propriedade e/ou tratadas pelo **Digiteam**, por meio de políticas, processos e procedimentos condizentes com o porte e o modelo de negócio, observando os Princípios de Segurança da Informação e a Lei Geral de Proteção de Dados (LGPD). Este documento busca, também, orientar a execução das ações relacionadas ao tratamento de dados, pessoais ou não, e o uso adequado de ativos e/ou informações pelos colaboradores, estagiários, terceiros, fornecedores, parceiros e outras partes envolvidas nos negócios da empresa.

2. ABRANGÊNCIA

Esta **Política** será aplicável a todos os colaboradores, terceiros e quaisquer outras pessoas, sejam físicas ou jurídicas, que tenham ou venham a ter acesso às Informações de propriedade e/ou tratadas pelo **Digiteam**.

3. LOCAL E DISPONIBILIDADE

Este documento está disponível para consulta em formato digital em: Sobre o Digiteam

4. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

A **Segurança da Informação** baseia-se na "preservação da confidencialidade, integridade e disponibilidade da informação". Esses três conceitos são considerados como Princípios de Segurança da Informação e devem ser garantidos e respeitados por todos aqueles sujeitos a esta política, considerando os seguintes conceitos:

- **Confidencialidade.** Garantia de que somente pessoas previamente autorizadas e selecionadas pelo **Digiteam** terão acesso às informações.

- **Disponibilidade.** Os dados poderão ser acessados e modificados pelos Titulares a qualquer momento. Além disso, deve ser assegurado que os dados estão disponíveis aos Colaboradores autorizados do **Digiteam**, de modo a garantir o cumprimento dos serviços contratados pelo titular.

- **Integridade.** Adoção das medidas necessárias a garantir a integridade dos dados e a manutenção de sua originalidade e conteúdo, de forma a assegurar a confiabilidade dos dados coletados e tratados pelo **Digiteam**.

5.ESTRUTURA ORGANIZACIONAL E ATRIBUIÇÕES

5.1. Diretoria

- Aprovar e garantir a manutenção e aplicação desta **Política**;

- Garantir aos demais departamentos os recursos necessários para atendimento a esta política e para a proteção dos dados sob a responsabilidade do **Digiteam**.

5.2. Departamento Administrativo/Financeiro

- Coletar a ciência por parte de todos os envolvidos em relação à existência e necessidade de cumprimento desta **Política** e manter em arquivo;

- Definir em conjunto com diretores e/ou gestores quando necessário, a adoção de sanções em caso de violação a esta Política.

5.3. Responsáveis pela tecnologia da informação / Departamento de Tecnologia da Informação (TI)

Os responsáveis pela tecnologia da informação do **Digiteam** têm como atribuições, relacionadas à presente política:

- Gerir e supervisionar a Segurança da Informação no âmbito do **Digiteam**

- Monitorar e avaliar periodicamente o plano estratégico de Segurança da Informação;

- Conduzir apurações em caso de suspeita ou ocorrência de incidentes em Segurança da Informação.

5.4. Demais sócios, colaboradores, prestadores de serviços do Digiteam

Cabe aos sócios, colaboradores, prestadores de serviços do **Digiteam**:

- Conhecer e cumprir rigorosamente esta **PSI**, bem como normas/procedimentos relacionados;
- Estar atento e reportar o **Digiteam** em caso de perceber ou suspeitar práticas em não conformidade com esta Política.

6. DIRETRIZES

Esta **PSI** estabelece diretrizes para o tratamento de Informações no decorrer das atividades dos integrantes do **Digiteam**. Estas orientações são complementares às instruções e procedimentos padrão de cada setor do **Digiteam**, como forma de garantir a atividade empresarial com a devida proteção das informações.

6.1. Diretrizes Gerais

Para fins desta Política ficam estabelecidas as seguintes diretrizes gerais:

a. **Propriedade da Informação:** toda informação gerada, adquirida, manuseada, armazenada, transportada e/ou descartada nas dependências e/ou em ativos da empresa deverá ser considerada patrimônio do **Digiteam** e utilizada exclusivamente para os interesses corporativos.

b. **Gerenciamento de acesso à informação:** O acesso lógico, o controle de acesso físico e o uso da informação do **Digiteam** devem ser aprovados, controlados, registrados, armazenados e monitorados, de forma a permitir a adequada execução das tarefas inerentes ao seu cargo ou função.

c. **Gestão de Incidentes:** todos os colaboradores, consultores e prestadores de serviço do **Digiteam**, em qualquer vínculo, função ou nível hierárquico têm a obrigação de reportar imediatamente quaisquer incidentes de segurança que tomarem conhecimento, de modo que possam ser registrados, avaliados e tratados de acordo com o plano de resposta a incidentes a ser definido.

d. **Treinamento e Conscientização:** deve ser estabelecido programa de conscientização, educação e treinamento, com o objetivo de disseminar a cultura de segurança da informação no **Digiteam**.

7. POLÍTICAS INTERNAS

7.1. Controle e gerenciamento de acesso

Para acesso dos dados e sistema interno do **Digiteam**, é obrigatório o uso de uma única identificação (login) e de senha de acesso fornecidos pelo **Departamento de Tecnologia da Informação (TI)**.

As permissões de acesso do **Colaborador** devem ser definidas pelo responsável por cada departamento do qual o **Colaborador** fizer parte, limitando-se a atividades estritamente necessárias à realização de suas tarefas. As permissões serão validadas e aprovadas por responsável pela área de Tecnologia indicado pela empresa.

Após o encerramento das atividades do **Colaborador**, seus acessos deverão ser bloqueados imediatamente.

Todos os logins e senhas são, obrigatoriamente, de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados quando constatada eventual irregularidade.

Os acessos a sistemas, diretórios, banco de dados e afins que contenham dados pessoais de **Usuários** ou clientes de clientes deverão ser acessados mediante a utilização de senhas fortes.

As senhas fortes deverão adotar o seguinte padrão:

Login:	e-mail corporativo
Senha:	No mínimo 8 caracteres, contendo pelo menos um caractere numérico, uma letra maiúscula e um caractere especial.

Sempre que possível, deverá ser habilitada autenticação multifatorial para maior segurança.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários, como no caso de mudança de função ou rescisão do contrato.

Os **Colaboradores** nomeados como Usuários Administradores poderão ter acesso aos equipamentos dos colaboradores. Por outro lado, nenhum usuário, incluindo os administradores, deverá ter acesso às senhas cadastras de outros usuários.

7.2. Política de uso aceitável

Informações armazenadas em dispositivos eletrônicos e computadores, sejam de propriedade do **Digiteam**, alugados pelo funcionário ou de terceiros, permanecem como propriedade exclusiva da empresa.

O colaborador deverá comunicar prontamente o roubo, a perda ou a divulgação não autorizada de informações.

Para fins de segurança e manutenção de rede, pessoas autorizadas pelo **Digiteam** podem monitorar equipamentos, sistemas e tráfego de rede a qualquer momento, de acordo com esta política.

7.2.1. Segurança

Todos os dispositivos de computação devem ser protegidos com uma tela de bloqueio protegida por senha com a função de ativação automática definida para 10 minutos ou menos.

O **Colaborador** deve bloquear a tela ou fazer logout quando o dispositivo estiver sem supervisão.

Os **Colaboradores** devem ter extrema cautela ao abrir anexos de e-mail recebidos de remetentes desconhecidos, que podem conter malware.

7.2.2. Uso inaceitável

As seguintes atividades são estritamente proibidas, sem exceções:

- Violações dos direitos de qualquer pessoa ou empresa protegidos por direitos autorais, segredos comerciais, patentes ou outras leis ou regulamentos de propriedade intelectual semelhantes, incluindo, mas não se limitando à instalação ou distribuição de produtos de software "pirateados" ou outros produtos de software que não estão devidamente licenciados para uso pelo **Digiteam**.

- Acesso a dados, a um servidor ou a uma conta para qualquer finalidade que não seja a condução de negócios.

- Exportar software, informações técnicas ou tecnologia em violação da legislação aplicável.

- Introdução de programas maliciosos na rede ou no servidor (por exemplo, vírus, worms, cavalos de Tróia, ransomware, etc.).

- Revelar a senha/frase de acesso a outras pessoas ou permitir o uso de sua conta por outras pessoas.

- Usar um ativo de computação para participar ativamente na aquisição ou transmissão de material que esteja em violação das leis de assédio sexual ou ambiente de trabalho hostil.

- Fazer ofertas fraudulentas de produtos, itens ou serviços.

- Causar violações de segurança ou interrupções na comunicação de rede.

- Contornar a autenticação do usuário ou a segurança de qualquer host, rede ou conta.

- Usar qualquer programa/script/comando ou enviar mensagens de qualquer tipo com a intenção de interferir ou desativar a sessão de terminal de um usuário, por qualquer meio, localmente ou via Internet/Intranet/Extranet.

- Fornecer informações sobre ou listas de funcionários ou clientes a partes externas do **Digiteam**.

7.3. Política de e-mail

O Colaborador deverá seguir as seguintes regras relacionadas ao e-mail profissional:

- Não abrir anexos com as extensões .bat, .exe, .src, .lnk e .com se não tiver certeza absoluta de que solicitou o e-mail.

- Desconfiar de todos os e-mails com assuntos estranhos e/ou em língua estrangeira.

- Não abrir ou encaminhar mensagens consideradas suspeitas ou caracterizadas como corrente, SPAM e *Phishing* (técnica de fraude online).

- Não utilizar o e-mail da empresa para assuntos pessoais.

7.4. Backup

- Os documentos devem ser salvos na rede ou nuvem;

- Os **Colaboradores** não estão autorizados a utilizar recursos (pen drive, cloud etc.) para efetuar backup;

- Deverá ser mantido controle rigoroso de acesso ao backup;

- O tempo de retenção deverá observar as necessidades da empresa, as especificidades do negócio e a legislação aplicável;

- A realização e manutenção de backup é uma atribuição exclusiva do **Departamento de Tecnologia da Informação (TI)**.

- O **Departamento Administrativo** poderá realizar o backup dos documentos relativos às informações financeiras e de departamento pessoal.

7.5. Instalação e uso de softwares

O **Departamento de Tecnologia da Informação (TI)** é responsável por homologar, controlar e manter os softwares utilizados na empresa, respeitando os direitos de propriedade intelectual.

Apenas softwares homologados e autorizados pelo **Departamento de Tecnologia da Informação (TI)** podem ser instalados nos equipamentos da empresa.

7.6. Descarte de mídia e documentos físicos

Deverá ser garantido que:

- As informações impressas e de conteúdo sensível sejam trituradas e ou incineradas.

- O descarte de recursos tecnológicos (ex: mídias, equipamentos etc.) seja realizado pelo **Departamento de Tecnologia da Informação (TI)**, mediante a utilização de técnicas que garantam a eliminação definitiva dos dados e a impossibilidade de sua recuperação.

7.7. Gestão de incidentes de segurança

Todos os incidentes ou fragilidades de Segurança da Informação devem ser reportados ao Departamento de Tecnologia, que deve proceder ao registro, análise e tratamento. Além disso, em caso de incidente de segurança envolvendo dados pessoais, aquele que suspeitar ou o identificá-lo também deverá reportar a ocorrência ao(à) Encarregado pelo tratamento de dados pessoais do

Digiteam (aqui) , nos termos da Política de Governança em Privacidade e Proteção de Dados Pessoais da empresa.

Convém que seja estabelecido um processo formal para gestão de incidentes de Segurança da Informação, definindo responsabilidades, hierarquia no tratamento, diretrizes de resposta a incidentes, entre outros pontos importantes.

8. VIGÊNCIA

Esta **Política**, aprovada pelo **Digiteam**, tem vigência imediata à data da sua aprovação e será revisada no período máximo de um 1 (um) ano ou havendo necessidade anterior, o que for menor, para que permaneça sempre atualizada.

DIGITEAM TECNOLOGIA LTDA:07821585000150
Assinado de forma digital por DIGITEAM TECNOLOGIA LTDA:07821585000150
Dados: 2024.02.09 11:29:50 -03'00'

OIKOS HOLDING E PARTICIPACOES LTDA:41818524000171
Assinado de forma digital por OIKOS HOLDING E PARTICIPACOES LTDA:41818524000171
Dados: 2024.02.09 11:30:08 -03'00'

DANIEL BORROTO:71178862186
Assinado de forma digital por DANIEL BORROTO:71178862186
Dados: 2024.02.09 11:30:21 -03'00'