Steffen & Effting
ADVOGADOS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS

DOCUMENTO	CLASSIFICAÇÃO	DATA	APROVADO POR:	VERSÃO
POL_001	Informação Interna	dd/mm/aaaa	[Nome]	1.0

1. INTRODUÇÃO

A empresa Palmeira Implementos Rodoviários entende que as informações corporativas são um bem essencial para suas atividades, e, através deste documento, pretende definir a Política que rege as operações relativas a estes dados.
Todas as informações aqui contidas se referem, doravante, à empresa Palmeira, como organização.

2. OBJETIVO

Estabelecer os conceitos e diretrizes relativos à Segurança da Informação e Proteção de Dados Pessoais, visando proteger as informações da organização, mantendo tal política alinhada aos objetivos estratégicos da empresa.

3. ESCOPO

Esta Política aplica-se a todos os colaboradores, estagiários, fornecedores, prestadores de serviço e visitantes das empresas da organização, incluídas as gerências de área, e a Direção da empresa.

Qualquer indivíduo ou empresa que tenha tido, tenha atualmente, ou venha a ter acesso a qualquer dado ou ativo de informação, considerado de propriedade da organização, em qualquer tempo, em qualquer circunstância, e em qualquer localização geográfica, estará sujeito ao determinado no presente documento.

4. CONCEITOS

A Segurança da Informação é aqui caracterizada pela preservação dos seguintes conceitos:

- **Confidencialidade:** Garante que o acesso às informações seja efetuado somente pelas pessoas autorizadas, durante o período necessário.

- **Integridade:** Garante que a Informação esteja íntegra e completa durante todo o seu ciclo de vida.

- **Disponibilidade:** Garante que a Informação esteja disponível para as pessoas autorizadas, sempre que se fizer necessária.

5. ESTRUTURA NORMATIVA

A estrutura normativa da Segurança da Informação da organização é composta pelos documentos relacionados a seguir:

- **Política:** define a estrutura, diretrizes e os papéis referentes à Segurança da Informação.

- **Normas e Padrões:** Estabelecem regras, definidas de acordo com as diretrizes da Política, a serem seguidas em diversas situações em que a Informação é tratada.

- **Procedimentos e Orientações:** Instrumentam as regras dispostas nas Normas, permitindo a direta aplicação nas atividades da organização.

5.1. Compliance com tratamento de dados pessoais

Todos os documentos desta estrutura, que necessitem consentimento para o tratamento de dados pessoais (definidos na Lei nro 13.709/2018 - LGPD) deverão incluir cláusula separada, em caráter inequívoco, que especifique dito tratamento, e que especifique o consentimento explícito do titular dos dados, de forma a dar cumprimento (*compliance*) com a correspondente Lei Geral de Proteção de Dados.

Sendo necessário o cumprimento com a GDPR (*General Data Protection Regulamentation*), a mesma deve ser também especificada, tendo cláusula específica.

6. DIRETRIZES

A seguir, são apresentadas as Diretrizes da Política de Segurança da Informação da organização. Estas Diretrizes devem ser a base fundamental para a elaboração de todas as Normas e Procedimentos.

6.1. Aspectos Gerais

- As informações (em formato físico ou lógico) e os ambientes tecnológicos utilizados pelos usuários são de exclusiva propriedade da organização, não podendo, sob nenhuma hipótese, ser interpretados como de uso pessoal;

- Excetuam-se desta propriedade, os dados pessoais compreendidos na Lei Geral de Proteção de Dados LGPD;

- Todos os colaboradores, estagiários, prestadores de serviço e visitantes devem ter ciência de que o uso das informações e dos sistemas de informação pode ser monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política e das Normas de Segurança da Informação, podendo estas servir de evidências para aplicações de medidas disciplinares processos administrativos e legais;

- Todo processo, sempre que possível, durante o seu ciclo de vida, deve garantir a segregação de funções, por meio de mais de uma pessoa ou equipe.

6.2. Tratamento da Informação

- Para assegurar a proteção adequada às informações, deve existir um método de classificação da informação de acordo com o grau de confidencialidade e criticidade para o negocio da organização;

- As informações devem ser atribuídas a um proprietário, formalmente designado como responsável pela autorização de acesso as informações sob sua responsabilidade;

- Dados Pessoais devem cumprir com todos os critérios da LGPD;

- Todas as informações devem estar adequadamente protegidas em observância às diretrizes de Segurança da Informação da organização em todo o seu ciclo de vida, que compreende: geração, manuseio, armazenamento, transporte e descarte;

- A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada ou gerada.

6.3. Gestão de acessos e Identidades

- O acesso às informações e aos ambientes tecnológicos da organização deve ser controlado de acordo com a sua classificação, de forma a garantir acesso apenas às pessoas autorizadas, mediante aprovação formal;

- Os acessos aos funcionários, estagiários, visitantes e prestadores de serviço devem ser solicitados, e aprovadas somente as informações necessárias ao desempenho de suas atividades.

6.4. Gestão de Incidentes de Segurança da Informação

Em caso de violação desta Política e Normas de Segurança da Informação:

- O Comitê Gestor de Segurança da Informação (CGSI) realizará deliberações somente nos incidentes classificados com alta criticidade. Após deliberação, o CGSI recomendará à Direção uma ação disciplinar a ser tomada;

- Todos os demais casos serão tratados pelo fluxo normal de resposta a incidentes

6.5. Partes Externas

Os contratos entre a organização e empresas fornecedoras e/ou prestadoras de serviços com acesso às informações, aos sistemas e/ou ao ambiente tecnológico da organização devem conter cláusulas que garantam a confidencialidade entre as partes e que assegurem minimamente que os profissionais sob sua responsabilidade cumpram a Política e as Normas de Segurança da Informação. Também devem cumprir rigorosamente com a LGPD.

7. RESPONSABILIDADES

7.1. Todos os Colaboradores, estagiários, visitantes, fornecedores e prestadores de serviço.

- Ler, Compreender, e cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da informação da organização, como também, quaisquer outras leis ou normas de segurança aplicáveis;

- Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a atual política, suas normas e procedimentos, a área de Gestão de Segurança de Informação da organização;

- Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados pela organização;

- Assegurar que os recursos tecnológicos, as informações e sistemas à sua disposição sejam utilizados apenas para as finalidades aprovadas pela organização;

- Cumprir as normas que regulamentam a propriedade intelectual;

- Não discutir assuntos confidenciais de trabalho em ambientes públicos ou áreas expostas (aviões, transporte, restaurantes, encontros sociais, etc.) incluindo a emissão de comentários e opiniões em blogs, páginas e redes sociais;

- Não compartilhar informações confidenciais de qualquer tipo;

- Comunicar imediatamente a área de Gestão de Segurança da Informação qualquer descumprimento ou violação desta política e/ou de suas Normas e Procedimentos, ou qualquer evento que coloque ou possa colocar em risco a segurança das informações da organização.

7.2. Gestores da Informação.

- Identificar, classificar e rotular as informações sob sua responsabilidade, de acordo com as normas da organização;

- Autorizar ou revogar os acessos à informações sob sua responsabilidade, revisando periodicamente os mesmos;

- Assumir a responsabilidade por todo o ciclo de vida da informação sob sua responsabilidade.

7.3. Área de Gestão de Segurança da Informação

- Prover todas as informações de Gestão de Segurança da Informação solicitadas pelo CGSI ou pela Diretoria Executiva;

- Prover ampla divulgação da Política e das Normas de Segurança da Informação para todos os colaboradores, estagiários, visitantes e prestadores de serviços;

- Promover ações de conscientização sobre Segurança da Informação para os colaboradores, estagiários, visitantes e prestadores de serviços;

- Propor projetos e iniciativas relacionadas ao aperfeiçoamento da Segurança da Informação da organização;

- Estabelecer procedimentos relacionados à instrumentação da Segurança da Informação da organização.

7.4. Comitê Gestor de Segurança da Informação

- Atuar como enlace fundamental entre a Direção da empresa e a Área de Gestão de Segurança da Informação, garantindo a fluidez da comunicação entre as mesmas;

- Reunir-se periodicamente ou extraordinariamente, analisando e tomando decisões sobre eventos e incidentes de Segurança da Informação;

- Observar as modificações políticas, estruturais e estratégicas da empresa, levando tais mudanças para que sejam refletidas na Política de Segurança da Informação.

7.5. Direção da Empresa

- Prover os recursos necessários para o cumprimento da Política de Segurança de Informação;

- Assegurar que a Política de Segurança da Informação é compatível com os objetivos e estratégias corporativas;

- Demonstrar liderança e comprometimento com a Política de Segurança da Informação, incentivando a sua aplicação, e dando o suporte moral e executivo para a execução da mesma;

- Assegurar que a Política de Segurança da Informação consegue atingir seus objetivos.

8. NÃO CONFORMIDADE

8.1. Definição

A Não conformidade está definida na presente Política como a violação, omissão, tentativa não consumada, ou ausência de cumprimento com quaisquer das definições, diretrizes, normas, procedimentos ou conceitos definidos nesta Política de Segurança da Informação, voluntária ou involuntariamente, por parte de um colaborador, estagiário, visitante, fornecedor ou prestador de serviços.

8.2. Determinação

- Qualquer colaborador, estagiário, visitante, fornecedor ou prestador de serviços pode denunciar uma suspeita de não conformidade com a Política de Segurança da Informação.

- A referida denúncia deve ser efetuada verbalmente, ou (preferentemente) por escrito, para a área de Gestão de Segurança de Informação, ou para um gestor de qualquer área da empresa, que, a sua vez, deve encaminhar a denúncia à área de Gestão de Segurança da Informação da organização.

- O formato da denuncia escrita deve estar definido nas Normas e Procedimentos da Segurança da Informação.

- Dispositivos e procedimentos de monitoramento e verificação de Segurança da Informação também podem indicar possíveis violações ou não cumprimentos. As formas de comunicação através destes dispositivos ou procedimentos devem estar definidas nas Normas e Procedimentos da Segurança da Informação.

- A Determinação final sobre a procedência da suspeita, ou veracidade das informações relativas à Segurança a Informação cabe somente ao responsável pela Gestão de Segurança da Informação.

8.3. Ação

As regras que estabelecem o controle e o tratamento de situações de não conformidade relativas à Política de Segurança da Informação da organização devem ser tratadas conforme a Política de Gestão de Riscos

Corporativos Vigente, ou conforme as leis vigentes no país, que regulamentem as punições correspondentes ao evento.

Na ocorrência de violação desta Política ou das Normas de Segurança da Informação, a Diretoria Executiva poderá adotar, com apoio das Gerências jurídicas e de Recursos Humanos, sanções administrativas e/ou legais, conforme os parágrafos a seguir:

8.3.1. Colaboradores e Estagiários

As punições serão aplicadas conforme análise do Comitê Gestor da Segurança da Informação, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência, e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho;

8.3.2. Fornecedores, Terceiros contratados ou Fornecedores de Serviço

O CGSI deverá analisar a situação, e deliberar sobre a aplicação de sanções previstas em contrato;

8.3.3. Visitantes

O CGSI deverá analisar a situação, e deliberar sobre a aplicação de sanções coerentes ao fato, respeitando as demais legislações vigentes.;

Para os casos de violações que impliquem em atividades ilegais, ou que possam incorrer em danos a organização, o infrator será responsabilizado pelos prejuízos, cabendo a aplicação das medidas judiciais pertinentes, sem prejuízo ao estipulado nos itens anteriormente descritos.

9. CASOS OMISSOS

O presente documento, e a totalidade dos responsáveis citados no mesmo, devem considerar que a tecnologia e as ameaças à Segurança da Informação se intensificam e se atualizam todos os dias.

Portanto, não se constitui rol enumerativo, sendo obrigação do usuário da organização adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir a proteção às informações da empresa.
Os eventuais casos que não estejam contemplados neste documento, ou nos documentos auxiliares que o compõem, devem ser analisados,

em primeira instância, pelo Gestor de Segurança da Informação, e, caso o mesmo não tenha uma solução ou medida plausível para o evento, caberá ao Comitê Gestor de Segurança da Informação, decidir o procedimento para cada caso específico.

10. ALTERAÇÕES

Este documento poderá conter eventuais erros de tipografia, ortografia ou gramática. Em tais casos, o responsável pela elaboração e manutenção poderá elaborar novas versões deste documento, com as devidas correções, sem a necessidade de nenhuma comunicação prévia aos interessados.

Demais alterações serão aplicadas à novas versões, sendo que novos acordos, reconhecimentos ou compromissos assumidos com respeito à este documento, farão sempre referência à versão mais recente do mesmo.

11. REVISÕES

Esta política será revisada anualmente, ou a qualquer momento em que o determine o Comitê Gestor de Segurança da Informação.

12. DEFINIÇÕES

Informação: Dados (eletrônicos ou físicos), ou registros de um sistema, devidamente processados.

- Dados Pessoais: Dados específicos a um indivíduo, definidos através da LGPD.

- Tratamento de Dados: Toda a operação realizada com dados, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

- Titular dos Dados: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

- Ativo: Tudo aquilo que possui ou constitui valor para a organização.

- Ativos de Informação: Conjunto de informações, armazenado de modo que possa ser identificado e reconhecido como valioso para a empresa. Trata-se de patrimônio intangível da empresa, constituído por suas informações de qualquer natureza, incluindo aquelas de caráter estratégico, técnico, administrativo, mercadológico, financeiro, de recursos humanos ou legais, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, compra, licenciamento, ou confiadas a organização por funcionários, parceiros, clientes, fornecedores, terceiros, em formato escrito, verbal, físico, digitalizado, que seja armazenado, transitado ou trafegado pelas estruturas da empresa, além de documentos em suporte físico ou mídia eletrônica que transitarem interna ou externamente a estrutura física da empresa.

- Sistemas de Informação: Sistemas computacionais utilizados pela empresa para suportar suas operações. Podem haver exceções que, mesmo não sendo sistemas informáticos, suportem operações da empresa.

- Ameaça: Causa potencial de um acidente, que possa vir a comprometer ou prejudicar da organização. Confidencialidade: Garante que o acesso às informações seja efetuado somente pelas pessoas autorizadas, durante o período necessário.

- Integridade: Garante que a Informação esteja íntegra, exata e completa durante todo o seu ciclo de vida.

- Disponibilidade: Garante que a Informação esteja disponível para as pessoas ou organismos autorizados, sempre que se fizer necessária.

- Risco de Segurança da Informação: Efeito da incerteza sobre os objetivos de Segurança da Informação da organização.

- Controle: medida de segurança adotada pela organização, para tratamento de um risco específico.

- Segregação de Funções: Consiste na separação entre as funções de autorização, aprovação de operações, execução, Controle e contabilização, de maneira que nenhum colaborador, visitante, estagiário ou

prestador de serviços, detenha poderes e atribuições em desacordo com este princípio, ou conflitantes entre si.

- Informações da Organização: Ativos de Informação que se relacionem diretamente à organização, suas atividades, dados de clientes, fornecedores, funcionários, estagiários, visitantes ou terceiros, e qualquer tipo de dado ou informação gerada ou alterada por membros da empresa, no exercício de suas funções.

- Comitê Gestor de Segurança da Informação: grupo multidisciplinar composto por membros das diretorias executivas, com o objetivo de avaliar a estratégia e diretrizes da Segurança da Informação seguidas pela empresa.

- LGPD Lei Geral de Proteção de Dados: Lei brasileira de número 13709/18, promulgada em 14 de agosto de 2018, que define as normas e procedimentos para o tratamento de dados pessoais.