Política de Segurança da Informação

10-A-DOC-LGPD

SÚMARIO

1 INTRODUÇÃO

A informação é um dos princípios ativos do mundo dos negócios. O uso correto da informação é capaz de criar vantagens competitivas, garantir o sucesso e a perpetuidade de uma empresa. Dada a importância, as informações são alvo de constantes ameaças internas e externas. As informações quando não utilizadas de forma adequada, geram riscos e podem causar prejuízos e ameaças a continuidade dos negócios.

Este documento define a política de segurança da informação das empresas da Moreia.

Como uma empresa moderna e voltada para o futuro, as empresas da Moreia reconhecem a necessidade de garantir que seus negócios operem sem problemas e sem interrupções, isto, para o benefício de seus clientes e outras partes interessadas.

Para fornecer tal nível de operação contínua, as empresas da Moreia implementaram um conjunto de controles de segurança da informação para tratar os riscos identificados.

A segurança da informação tem muitos benefícios para o negócio, incluindo:

- Proteção de fluxos de receita e lucratividade da empresa
- Garantir o fornecimento de bens e serviços aos clientes
- Manutenção e aprimoramento do valor do negócio
- Cumprimento dos requisitos legais e regulamentares

2 OBJETIVO

Estabelecer diretrizes que permitam aos Colaboradores da Moreia seguirem padrões de comportamento e conduta relacionados à segurança da informação e proteção de dados, adequados às necessidades do negócio e de proteção legal das empresas e dos indivíduos. Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações da Moreia quanto à:

- **Integridade**: consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação às inserções, alterações, exclusões e processamentos, com a garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

- **Confidencialidade**: a informação só pode ser acessada, manuseada e atualizada por pessoas devidamente credenciadas.

- **Ética**: assegurar que as informações sejam utilizadas dentro dos preceitos aqui estabelecidos e em hipótese alguma, violando as normas internas desta política ou das leis vigentes.

- **Sigilo**: assegurar que as informações sejam utilizadas apenas para finalidade autorizada.

- **Autenticidade**: garantia da veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações.

3 ABRANGENCIA

Esta política se aplica a todas as operações, pessoas e processos que constituem os sistemas de informações da organização, incluindo membros do conselho, diretores, funcionários, fornecedores e outros terceiros que têm acesso aos sistemas das empresas da Moreia.

4 COMITÊ GESTOR DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO:

- Membro da Diretoria;
- Gerente de Informática;
- Gerente de Controladoria;
- Gerente Financeiro;
- Gerente de Recursos Humanos;
- Assessoria Jurídica

Contato: segurancadainformacao@moreiaparts.com.br
Telefone (11)3616-0756 | Ramal: 10756

Os documentos de suporte a seguir são relevantes para esta política de segurança da informação e fornecem esclarecimentos adicionais sobre como ela é aplicada:

- *Política de Computação em Nuvem*
- *Política de Dispositivos Móveis*
- *Política de Controle de Acesso*
- *Política Criptográfica*
- *Política de Segurança Física*
- *Política Antimalware*
- *Política de Segurança de Rede*
- *Política de Mensagens Eletrônicas*
- *Política de Retenção e Proteção de Registros*
- *Política de Proteção de Dados*

5 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

5..1 Requisitos de segurança da informação

Uma definição clara dos requisitos para a segurança da informação das empresas da Moreia será acordada e mantida com os clientes internos do negócio e do serviço em nuvem, de modo que toda a atividade de segurança da informação seja focada no cumprimento desses requisitos. Requisitos estatutários, regulatórios e contratuais também serão documentados e inseridos no processo de planejamento. Requisitos específicos com relação à segurança de sistemas ou serviços novos ou alterados serão identificados em cada projeto.

É um princípio fundamental do programa de segurança da informação das empresas da Moreia que os controles são implementados em razão da necessidade do negócio, e isso será comunicado regularmente a todos os funcionários por meio de reuniões de equipe e documentos informativos.

5..2 Quadro de configuração dos objetivos

Um ciclo regular será usado para a definição de objetivos de segurança da informação, para coincidir com o ciclo de planejamento orçamentário. Isso garantirá que um financiamento adequado seja obtido para as atividades de melhoria identificadas. Esses objetivos serão baseados em uma compreensão clara dos requisitos do negócio, informados pelo processo de revisão da administração, durante o qual as visões das partes interessadas podem ser obtidas.

Objetivos de segurança da informação serão documentados por um período de tempo, juntamente com detalhes de como eles serão alcançados. Estes serão avaliados e monitorados como parte das revisões de gestão para garantir que eles permaneçam válidos. Se forem necessárias emendas, elas serão gerenciadas por meio do processo de gerenciamento de mudanças.

Os controles de segurança da informação serão adotados, quando apropriado, pelas empresas da Moreia. Estes serão revistos regularmente considerando o resultado das avaliações de risco e de acordo com os planos de tratamento de riscos de segurança da informação.

Além disso, controles aprimorados e adicionais de códigos serão adotados e implementados quando apropriado. A adoção desses códigos fornecerá garantia adicional aos nossos clientes e ajudará ainda mais com nossa conformidade com a legislação de proteção de dados.

5..3 Melhoria contínua da segurança da informação

A política das empresas da Moreia em relação à melhoria contínua é:

- Melhorar continuamente a eficácia dos controles de segurança da informação;
- Aprimorar os processos atuais para adequá-los às boas práticas, conforme definido;
- Aumentar o nível de proatividade (e a percepção da proatividade das partes interessadas) em relação à segurança da informação;
- Tornar os processos e controles de segurança da informação mais mensuráveis, para fornecer uma base sólida para decisões;
- Revisar métricas relevantes anualmente para avaliar se é apropriado alterá-las, com base nos dados históricos coletados;
- Obter ideias para melhoria por meio de reuniões regulares e outras formas de comunicação com as partes interessadas;
- Analisar ideias para melhoria nas reuniões regulares de gestão, a fim de priorizar e avaliar prazos e benefícios.

Ideias para melhorias podem ser obtidas de qualquer fonte, incluindo funcionários, clientes, fornecedores, equipe de TI, avaliações de risco e relatórios de serviço. Uma vez identificados, elas serão registradas e avaliadas em revisões administrativas.

5..4 Conjuntos de políticas de segurança da informação

As empresas da Moreia definem a política em uma ampla variedade de áreas relacionadas à segurança da informação, descritas em detalhes em um conjunto abrangente de políticas que acompanha este documento.

Cada uma dessas políticas é definida e acordada por uma ou mais pessoas com competência na área específica e, uma vez formalmente aprovada, é comunica ao público-alvo, dentro e fora da organização.

A tabela abaixo mostra as políticas individuais, resume o conteúdo de cada política e o público-alvo das partes interessadas.

Título da política	Áreas endereçadas	Público-alvo
Política de Computação em Nuvem	Diligências, configuração, gerenciamento e remoção de serviços de computação em nuvem.	Funcionários envolvidos na aquisição e gerenciamento de serviços em nuvem
Política de Dispositivos Móveis	Segurança de dispositivos móveis, como laptops, tablets e smartphones, fornecidos pela organização ou pelo indivíduo para uso comercial.	Usuários de dispositivos móveis fornecidos pela empresa ou próprio dispositivo do funcionário
Política de Controle de Acesso	Registro de usuário e cancelamento de registro, fornecimento de direitos de acesso, acesso externo, revisões de acesso, política de senha, responsabilidades do usuário e controle de acesso ao sistema e ao aplicativo.	Funcionários envolvidos na configuração e gerenciamento do controle de acesso
Política Criptográfica	Avaliação de risco, seleção de técnica, implantação, teste e revisão de criptografia e gerenciamento de chaves	Colaboradores envolvidos na criação e gestão do uso de tecnologia e técnicas criptográficas
Política de Segurança Física	Áreas de segurança local, segurança de papel e equipamento e gerenciamento do ciclo de vida de equipamentos	Todos os funcionários
Política Antimalware	Firewalls, antivírus, filtragem de spam, instalação e verificação de software, gerenciamento de vulnerabilidades, treinamento de conscientização do usuário, monitoramento e alertas de ameaças, revisões técnicas e gerenciamento de incidentes de malware.	Funcionários responsáveis por proteger a infraestrutura da organização contra malware
Política de Segurança de Rede	Projeto de segurança de rede, incluindo segregação de rede, segurança de perímetro, redes sem fio e acesso remoto; gerenciamento de segurança de rede, incluindo funções e responsabilidades, registro e monitoramento e alterações.	Funcionários responsáveis por projetar, implementar e gerenciar redes
Política de Mensagens Eletrônicas	Envio e recebimento de mensagens eletrônicas, monitoramento de facilidades de mensagens eletrônicas e uso de e-mail.	Usuários de facilidades de mensagens eletrônicas
Política de Retenção e Proteção de Registros	Período de retenção para tipos de registro específicos, uso de criptografia, seleção de mídia, recuperação de registros, destruição e revisão.	Empregados responsáveis pela criação e gestão de registros
Política de Proteção de Dados	Legislação, definições e requisitos de proteção de dados aplicáveis.	Funcionários responsáveis por projetar e gerenciar sistemas usando dados pessoais

Tabela 1 – Conjunto de documentos de política

5..5 Aplicação da política de segurança da informação

As declarações de políticas feitas neste documento e no conjunto de políticas de suporte listadas na *Tabela 1* foram revisadas e aprovadas pela alta direção das empresas da Moreia e devem ser cumpridas. A falha de um funcionário em cumprir essas políticas pode resultar na tomada de medidas disciplinares de acordo com o processo interno da organização.

Perguntas relacionadas a qualquer política das empresas da Moreia deve ser abordada, em primeira instância, ao supervisor imediato do funcionário.

6 RECOMENDAÇÕES PARA O USO DOS RECURSOS :

A informação deve ser adequadamente manuseada e protegida e pode estar presente em diversas formas, tais como: planilhas, aplicações, relatórios, consultas sistêmicas, diretórios de rede, bancos de dados, mídia impressa, magnética ou ótica, dispositivos eletrônicos, equipamentos portáteis, microfilmes e até mesmo por meio da comunicação oral. Toda informação gerada, manuseada ou desenvolvida pela Moreia, constitui ativo da empresa, sendo essencial à condução de negócios e em última análise, à sua existência. Independente da forma apresentada ou do meio pelo qual é compartilhada deve ser utilizada unicamente para a finalidade autorizada. A modificação, divulgação e destruição não autorizadas, mesmo que oriundas de erros, fraudes, vandalismo, espionagem ou sabotagem, podem causar danos, inclusive financeiros, aos negócios da Moreia.

Somente atividades lícitas, éticas e administrativamente devem ser realizadas, pelo usuário, no âmbito da infraestrutura de TI. Os sistemas de TI deverão ser utilizados sem violação dos direitos de propriedade intelectual de qualquer pessoa ou empresa, como marcas e patentes, nome comercial, segredo empresarial, domínio na Internet ou qualquer outro material, que não tenha autorização expressa do autor ou proprietário dos direitos.

São confidenciais, quaisquer informações não disponíveis ao público ou reservadas, dados, especificações técnicas, desenhos, manuais, esboços, modelos, projetos, estudos, protótipos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em qualquer meio, programas ou documentações de computador, comunicações por escrito ou verbais ou ainda qualquer outra forma de domínio da Moreia.

O usuário ao ter acesso a informações confidenciais, deverá mantê-las e resguardá-las em caráter sigiloso, bem como, limitar seu acesso, controlar quaisquer cópias de documentos, dados e reproduções que porventura sejam extraídas da mesma. Nenhuma das informações confidenciais podem ser repassadas para terceiros sem consentimento por escrito do Diretor responsável pela unidade de negócios. As informações confidenciais somente poderão ser utilizadas para fins de execução das atividades exercidas pelo usuário. O usuário deverá resguardar as informações confidenciais de forma estrita, e não revelá-las, a pessoas não autorizadas. A parte que receber as informações será responsável por qualquer descumprimento desta Política.

6..1 Práticas recomendadas

Desta forma, recomenda-se aos usuários a adoção das seguintes práticas:

- Utilizar criptografia sempre que enviar ou receber dados com informações sensíveis;
Certificar a procedência do sítio e a utilização de conexões seguras (criptografadas) ao realizar transações via web;

- Verificar se o certificado do site ao qual se deseja acessar é íntegro e corresponde realmente aquele site, observando ainda, se o mesmo está dentro do prazo de validade;
- Certificar que o endereço apresentado no navegador corresponde ao sítio que realmente quer acessar, antes de realizar qualquer ação ou transação;
- Digitar no navegador o endereço desejado e não utilizar links como recurso para acessar um outro endereço destino;
- Não abrir arquivos ou executar programas anexados a e-mails, sem antes verifica-los com um antivírus;
- Não utilizar o formato executável em arquivos compactados, pois estes tipos são propícios à propagação de vírus.

6..2 Recomendações sobre atividades permitidas:

- Utilizar programas de computador licenciados para uso, de acordo com as disposições específicas previstas em contrato. A instalação de programas e sistemas homologados é atribuição da administração de sistemas e TI;
- Criar, transmitir, distribuir, disponibilizar e armazenar documentos, desde que respeite às leis e regulamentações, notadamente àqueles referentes aos crimes informáticos, ética, decência, pornografia envolvendo crianças, honra e imagem de pessoas ou empresas, vida privada e intimidade.

6..3 Recomendações sobre atividades não permitidas:

-Introduzir códigos maliciosos nos sistemas da Moreia;
-Revelar códigos de identificação, autenticação e autorização de uso pessoal (conta, senhas, chaves privadas etc) ou permitir o uso por terceiros de recursos autorizados por intermédio desses códigos;
-Divulgar ou comercializar produtos, itens ou serviços a partir de qualquer recurso dos sistemas da Moreia;
-Tentar interferir sem autorização em um serviço, sobrecarregá-lo ou, ainda, desativá-lo, inclusive aderir ou cooperar com ataques de negação de serviços internos ou externos;
-Alterar registro de evento dos sistemas, informações ou dados;
-Modificar qualquer dado, configuração, protocolos de comunicação, sem a expressa autorização;
-Obter acesso não autorizado, ou acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades nos sistemas da Moreia;
-Monitorar ou interceptar o tráfego de dados nos sistemas sem as devidas autorizações;
-Violar medida de segurança ou de autenticação, sem as devidas autorizações;
-Fornecer informações a terceiros, sobre usuários ou serviços disponibilizados nos sistemas da Moreia, exceto os de natureza pública ou mediante autorização de autoridade competente;
-Fornecer dados classificados como sigilosos, sem as devidas autorizações;
-Compartilhamento de informações sensíveis do negócio;
-Divulgação de informações de clientes e das operações contratadas;
-Divulgação de dados restritos de colaboradores;
-Envio de e-mail (interno ou externo) com informações cadastrais, sejam de funcionário ou clientes;
-Envio de informações da Moreia para endereços particulares de e-mail;
-Utilizar uma impressora coletiva para gerar informações confidenciais e não recolher o documento impresso imediatamente;
-Discutir ou comentar assuntos confidenciais em locais públicos;
-Discutir ou comentar assuntos confidencias com pessoas não autorizadas;
-Utilizar as informações da Moreia para obter ganhos pessoais;

-Armazenamento ou uso de jogos em computador ou sistema informacional da Moreia.

7 RESPONSABILIDADES:

7..1 Geral

De forma geral, compete a todos Usuários:
- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação da Moreia;
- Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados pela Moreia;
- Assegurar que os recursos tecnológicos, as informações e sistemas a sua disposição sejam utilizados apenas para as finalidades aprovadas pela Moreia;
- Cumprir as leis e as normas que regulamentam a propriedade intelectual;
- Não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (aviões, transporte, restaurantes, encontros sociais etc.) incluindo a emissão de comentários e opiniões em blogs e redes sociais;
- Não compartilhar informações confidenciais de qualquer tipo;
- Comunicar imediatamente à área de Gestão de Segurança da Informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos;
- Política de tela limpa. Se a pessoa não estiver no local de trabalho, todos os documentos em papel e todas as mídias de armazenamento de dados classificadas como confidenciais devem ser removidas da mesa ou de outros locais (impressoras, máquinas de fax, copiadoras, etc.) para evitar o acesso não autorizado.

7..2 Uso da Internet:

A Internet pode ser acessada somente por meio da rede local da organização com a infraestrutura adequada e proteção do firewall. O acesso direto à Internet por meio de modem, acesso móvel à Internet, rede sem fio ou outros dispositivos de acesso direto à Internet convém que seja autorizado pelo gestor da área em caso de falha no link de internet da entidade. O uso de Internet deve ser apenas através da arquitetura segura definida pela área de Tecnologia, utilizando-se de recursos firewall (software que serve como parede de proteção contra invasões externas à rede local). O usuário não deve alterar a configuração do navegador da sua máquina no que diz respeito aos parâmetros de segurança. Havendo necessidade, a Assessoria de Informática deve ser acionada para informar o procedimento a ser seguido.

É proibido:
- visualização, transferência, cópia ou qualquer outro tipo de acesso a sites: de conteúdo pornográfico, bem como a distribuição, interna ou externa, de qualquer tipo de conteúdo proveniente destes sites; que defendam atividades ilegais; o que menosprezem, depreciem e incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, religião, nacionalidade.
- A transferência ou cópia de arquivos de vídeo, som, ou quaisquer outros tipos de arquivos que não sejam relacionados aos interesses de negócios da Moreia. Este tipo de ação afeta diretamente os recursos de rede.

Participação em:

- salas de chat ou grupos de discussão de assuntos não relacionados aos negócios da Moreia; ou qualquer discussão pública sobre os negócios da Moreia, através do uso de salas de chat, grupos de discussão, ou qualquer outro tipo de fórum público, a menos que autorizado. A área de tecnologia pode bloquear o acesso a algumas páginas da Internet para usuários, grupos de usuários ou todos os funcionários da organização.
- O usuário é responsável por todas as consequências possíveis que surjam do uso não autorizado ou inadequado dos serviços ou do conteúdo da Internet. O ambiente de internet deve ser usado para o desempenho das atividades profissionais do Usuário. Sites que não contenham informações que agreguem conhecimento profissional para o negócio não devem ser acessados. Os acessos realizados nesse ambiente são monitorados pelo TI com o objetivo de garantir o cumprimento dessa política. A Moreia se reserva ao direito de supervisionar o uso de todos os seus serviços de computação, pois o acesso ao Ambiente de Internet é oferecido pela entidade para condução das atividades do negócio e auxílio no dia-a-dia das atividades profissionais, devendo ser utilizada de maneira eficaz e pró-ativa. O acesso à Internet só será permitido aos sites liberados e autorizados, e poderá ser monitorado pela Assessoria de Informática. A entidade se reserva ao direito de bloquear, sem aviso prévio, o acesso a sites cujo conteúdo não seja pertinente aos negócios da Moreia.

7..3 E-mail e outros métodos de troca de mensagens:

Os usuários só podem enviar mensagens que contenham informações verdadeiras. Não pode originar ou encaminhar mensagens ou imagens que contenham: declarações difamatórias ou linguagem ofensivas de qualquer natureza; menosprezem, depreciem ou incitem ao preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade ou deficiência física; possua informação pornográfica, obscena ou imprópria para um ambiente profissional; possam trazer prejuízo a outras pessoas; sejam hostis ou inúteis; que defendam ou possibilitem a realização de atividades ilegais; sugira a formação ou divulgação de correntes de mensagens; possam prejudicar a imagem da Moreia ou de outras organizações.

8 PENALIDADES

Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas, pelo Usuário, no âmbito da infraestrutura de TI, ficando os transgressores sujeitos sanções da Lei Penal, Civil e Administrativa, na medida da conduta, dolosa ou culposa, que praticarem.

Para os colaboradores, pode acarretar na aplicação de advertência e/ou suspensão ou desligamento formal.
Para os prestadores de serviços, na aplicação rescisória imediata do respectivo contrato violado, ficando sujeito as penalidades civil e penal, e se o caso, indenização por danos moral e material.

9 ACEITE da POLITICA:

Ao acessar dados, software, aplicativos e/ou Internet, fornecido pela Moreia, para execução de suas atividades, o Usuário concorda e aceita integralmente com as disposições desta Política de Segurança da Informação e Privacidade de Dados.