Política de Segurança da Informação – Engesoftware

1. Objetivo

Estabelecer diretrizes, responsabilidades e procedimentos para proteger as informações da Engesoftware contra ameaças internas e externas, minimizando os riscos à integridade, confidencialidade e disponibilidade das informações.

2. Âmbito

Aplica-se a todos os colaboradores, prestadores de serviço, consultores, estagiários e terceiros que tenham acesso aos ativos de informação, sistemas, redes e instalações da Engesoftware.

3. Princípios

Confidencialidade: Assegurar que informações sensíveis estejam acessíveis apenas para indivíduos com autorização.

Integridade: Preservar a precisão e a completude das informações e métodos de processamento.

Disponibilidade: Garantir que usuários autorizados tenham acesso oportuno e contínuo às informações e ativos.

4. Classificação da Informação

As informações serão classificadas de acordo com sua importância e nível de confidencialidade:

Pública: Informações que podem ser acessadas e divulgadas sem restrições, como conteúdo institucional ou dados já públicos.

Interna: Informações para uso exclusivo da Engesoftware e seus colaboradores. Ex: políticas internas, manuais de operação.

Confidencial: Informações que, se divulgadas, podem causar danos à empresa ou clientes. Ex: dados de clientes e contratos comerciais.

Restrita: Informações críticas que, se expostas, podem comprometer seriamente a empresa. Ex: dados financeiros e informações de segurança de sistemas.

5. Controle de Acesso

Princípio do Menor Privilégio: Acesso será concedido apenas conforme a necessidade para execução das tarefas.

Autenticação e Senhas: Senhas devem ser robustas (mínimo de 12 caracteres, contendo letras maiúsculas, minúsculas, números e caracteres especiais) e trocadas a cada 90 dias. É proibido o compartilhamento de senhas.

Autenticação Multifatorial (MFA): Todos os sistemas críticos e que contenham dados confidenciais devem adotar MFA como requisito de acesso.

Controle de Acesso Físico: Áreas sensíveis, como data centers e salas de servidores, devem ter controle de acesso restrito e registro de entradas e saídas.

6. Segurança Física e do Ambiente

Proteção de Equipamentos: Computadores e dispositivos móveis devem ser bloqueados quando não estiverem em uso. Equipamentos não devem ser deixados em áreas públicas sem supervisão.

Ambiente Seguro: Instalações críticas devem estar protegidas contra acesso não autorizado e desastres naturais. Inclui segurança contra incêndios, controle de temperatura e umidade, e sistemas de monitoramento.

Uso de Dispositivos Externos: É proibido o uso de dispositivos de armazenamento externo (USB, discos externos) sem autorização prévia do setor de segurança.

7. Proteção contra Malware e Ameaças Digitais

Antivírus e Ferramentas de Segurança: Todos os dispositivos devem ter antivírus atualizado, além de ferramentas de proteção contra malware e ransomware.

Atualizações e Patches de Segurança: Sistemas operacionais, aplicativos e dispositivos devem estar sempre atualizados com os patches de segurança mais recentes.

Política de Uso Aceitável: O acesso a sites não relacionados ao trabalho deve ser evitado, especialmente aqueles com conteúdo suspeito, e-mails suspeitos não devem ser abertos, devendo ser reportados imediatamente.

8. Gestão de Incidentes de Segurança da Informação

Procedimento de Resposta a Incidentes: A Engesoftware deve manter um plano formal de resposta a incidentes com ações para detecção, contenção, erradicação e recuperação.

Notificação de Incidentes: Todos os incidentes de segurança, incluindo tentativas de acesso não autorizado, devem ser reportados imediatamente ao setor de segurança da informação.

Análise Pós-Incidente: Após cada incidente, será realizada uma análise para identificar falhas e implementar ações corretivas, visando evitar recorrências.

9. Política de Backup e Recuperação de Desastres

Realização de Backups: Backups de sistemas e dados críticos devem ser realizados regularmente, com cópias armazenadas em locais distintos do ambiente principal.

Ciclo de Retenção: Backups devem seguir um ciclo de retenção que atenda às necessidades operacionais e regulatórias, mantendo cópias históricas conforme as exigências legais.

Teste de Backups: Backups devem ser periodicamente testados para garantir sua integridade e viabilidade de restauração.

Plano de Recuperação de Desastres (DRP): O DRP deve ser atualizado e testado anualmente, incluindo simulações de cenários de desastres que possam impactar as operações da empresa.

10. Conformidade com Normas e Regulamentos

Adequação à LGPD: Engesoftware compromete-se a proteger os dados pessoais em conformidade com a LGPD, adotando práticas de transparência, segurança e respeito aos direitos dos titulares.

Treinamento e Auditorias Regulares: Auditorias periódicas serão realizadas para avaliar a conformidade com esta política, bem como com normas externas relevantes, como ISO 27001.

Gestão de Terceiros: Todos os terceiros e fornecedores que tenham acesso a dados da empresa devem assinar um termo de confidencialidade e estar em conformidade com as políticas de segurança.

11. Treinamento e Conscientização

Treinamento Inicial e Recorrente: Todos os colaboradores devem passar por um treinamento inicial de segurança da informação ao ingressarem na empresa e por reciclagens periódicas, incluindo atualizações sobre ameaças emergentes.

Campanhas de Conscientização: Engesoftware deve realizar campanhas regulares sobre boas práticas de segurança, com conteúdos como e-mails, workshops e palestras.

Responsabilidade Individual: Todos os colaboradores têm a responsabilidade de proteger as informações da empresa e de reportar comportamentos suspeitos.

12. Auditoria e Monitoramento

Monitoramento Contínuo: Sistemas e redes devem ser monitorados continuamente para identificar atividades suspeitas ou potencialmente prejudiciais.

Auditorias Internas e Externas: Auditorias regulares devem avaliar a eficácia das políticas de segurança, com relatórios apresentados à alta administração para acompanhamento.

Análise de Logs: Logs de acessos e atividades devem ser registrados e analisados periodicamente para identificar anomalias ou atividades não autorizadas.

13. Política de Uso de Dispositivos Móveis e Trabalhos Remotos

Segurança de Dispositivos Móveis: Todos os dispositivos móveis devem ter criptografia de dados e proteção por senha. Dispositivos pessoais só poderão ser usados para acesso a informações da empresa mediante autorização.

Trabalho Remoto: Acesso remoto deve ser realizado exclusivamente por meio de soluções seguras e autorizadas, como VPN e MFA. Informações sensíveis não devem ser armazenadas em dispositivos pessoais.

14. Penalidades por Não Conformidade

Consequências Disciplinares: A não conformidade com esta política pode resultar em ações disciplinares, como advertências, suspensão, demissão ou ação legal.

Responsabilização: Cada colaborador é responsável pelo cumprimento desta política e por garantir que suas ações estejam em conformidade com os padrões de segurança.

15. Revisão e Atualização da Política

Revisões Periódicas: Esta política será revisada anualmente ou conforme necessário para assegurar que continua adequada às ameaças e requisitos regulamentares.

Responsabilidade pela Revisão: A equipe de segurança da informação é responsável por revisar e atualizar a política, reportando mudanças significativas à alta administração para aprovação.