1. OBJETIVOS

1.1. OBJETIVOS E METAS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- **Identificação e Avaliação de Riscos:** Identificar e avaliar os riscos de segurança da informação que a organização enfrenta, com o objetivo de priorizar e gerenciar os riscos de acordo com sua gravidade e impacto potencial;
- **Consciência e Treinamento:** Garantir que os funcionários e contratados da organização estejam conscientes dos riscos de segurança da informação e treinados para adotar boas práticas de segurança da informação;
- **Medidas Técnicas e Organizacionais:** Implementar medidas técnicas e organizacionais para garantir a confidencialidade, integridade e disponibilidade das informações da organização, como controles de acesso, criptografia, monitoramento e backup;
- **Conformidade Legal:** Garantir a conformidade com as leis e regulamentações aplicáveis, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (RGPD) na União Europeia;
- **Plano de Resposta a Incidentes:** Estabelecer um plano de resposta a incidentes de segurança da informação, para lidar com possíveis violações de segurança e minimizar seus impactos;
- **Auditorias Regulares:** Realizar auditorias regulares da PSI, a fim de avaliar a eficácia das medidas de segurança implementadas e identificar áreas que precisam de melhorias;
- **Cultura de Segurança:** Promover a cultura de segurança da informação em toda a organização, incentivando os funcionários a reportar quaisquer incidentes ou possíveis vulnerabilidades de segurança e criando um ambiente em que a segurança da informação seja uma prioridade para todos.

1.2. PRINCIPAIS AMEAÇAS E VULNERABILIDADE

A Engelmig se compromete a proteger todas as informações geradas e/ou consumidas por ela, utilizando meios tecnológicos avançados. Abaixo, destacam-se as principais ameaças e vulnerabilidades que a empresa enfrenta:

- ***Malware:*** programas maliciosos, como vírus, trojans e *ransomware*, que podem infectar os sistemas de informação e causar danos ou roubar informações confidenciais;
- ***Phishing:*** tentativas de enganar os usuários para obter informações confidenciais, como senhas e dados bancários, por meio de e-mails, mensagens de texto ou ligações telefônicas falsas;
- **Engenharia Social:** tentativas de manipular os usuários para obter informações confidenciais, como senhas, por meio de técnicas psicológicas, como falsas promessas, pretextos e intimidação;
- **Ataques de Negação de Serviço (*DDoS*):** ataques que sobrecarregam os sistemas de informação da empresa com tráfego de rede malicioso, tornando-os inacessíveis para usuários legítimos;
- **Acesso Não Autorizado:** acesso não autorizado aos sistemas de informação por usuários internos ou externos, que podem roubar informações ou causar danos aos sistemas;

- **Falhas de Segurança:** vulnerabilidades nos sistemas de informação que podem ser exploradas por hackers ou outros atores mal-intencionados para obter acesso ou roubar informações confidenciais;
- **Problemas de Configuração:** erros de configuração nos sistemas de informação que podem levar a vulnerabilidades de segurança;
- **Fraude:** fraudes internas ou externas que podem ser cometidas por funcionários ou terceiros, que podem roubar informações confidenciais ou causar danos aos sistemas;
- **Desastres Naturais ou Falhas de Energia:** desastres naturais, como incêndios, inundações ou terremotos, ou falhas de energia que podem causar danos físicos aos sistemas de informação ou interrupções no fornecimento de energia elétrica que podem afetar o funcionamento dos sistemas.

Essas ameaças podem ter impactos significativos, incluindo perda de dados, interrupção dos negócios, danos à reputação e perda financeira. Por isso, é importante implementar medidas de segurança eficazes para proteger os sistemas de informação da empresa.

2. IDENTIFICAÇÃO DOS RECUROS CRÍTICOS

2.1. A INFORMAÇÃO COMO PRINCIPAL ATIVO DA EMPRESA

A informação que circula na empresa é um ativo essencial. Isso inclui dados financeiros, estatísticas de acidentes, índices de absenteísmo e outras informações que são fundamentais para a geração de resultados e o atendimento aos anseios dos stakeholders. Portanto, toda informação gerada, consumida e/ou enviada durante os processos produtivos deve ser adequadamente protegida.

Cada funcionário da Engelmig tem um papel específico, desde as tarefas mais simples até os níveis mais altos de gestão. Todos utilizam recursos tecnológicos disponíveis para desempenhar suas funções. É essencial identificar as necessidades de cada funcionário para maximizar a eficácia desses recursos, seja por meio da instalação de softwares, concessão e revogação de acessos aos sistemas, ou fornecimento de ativos como computadores e celulares.

A cadeia hierárquica desempenha um papel importante na definição de entrega de recursos e liberação de acesso à informação, em alinhamento com esta Política de Segurança da Informação (PSI). Os líderes, com o suporte do Departamento de Tecnologia da Informação, devem determinar quais recursos são necessários para que seus liderados possam executar suas tarefas com eficiência.

Além disso, é importante reconhecer que a empresa possui recursos limitados, e as liberações de ativos devem respeitar um orçamento previamente aprovado pela Diretoria. No entanto, este orçamento pode ser ajustado em situações emergenciais e/ou imprevistas.

Melhoria Contínua

Para garantir a eficácia da Política de Segurança da Informação e a proteção dos recursos críticos, a Engelmig deve adotar práticas contínuas de avaliação e melhoria. Isso inclui a análise regular dos processos,

atualização de políticas e procedimentos, e treinamento contínuo dos funcionários para manter a segurança da informação como uma prioridade constante.

2.2. DADOS CONFIDENCIAIS

Informações confidenciais, como dados de clientes, informações financeiras e segredos comerciais, que precisam ser protegidos para garantir a privacidade e a segurança das informações da empresa.

O acesso e manipulação de tais informações depende do departamento/área do funcionário, além do nível deste (assistente, líder, gestor etc.). Garantir a privacidade e a segurança destes dados é assegurar que somente as pessoas autorizadas podem acessá-los, por quaisquer meios que sejam utilizados.

2.3. SISTEMAS DE PROCESSAMENTO DE DADOS

Sistemas que processam informações, como bancos de dados, servidores e aplicativos, que são essenciais para o funcionamento do negócio.

Para atender a todos os requisitos dos seus diretores e às necessidades internas, a Engelmig utiliza vários sistemas, como: ZEUS, SENIOR, Nasajon, Intranet e outros. Não é objetivo desta Política detalhar o funcionamento de cada sistema, mas sim identificar e explicar o os riscos envolvidos na utilização deles.

Estes Sistemas são atualmente hospedados na infraestrutura de nuvem da Oracle Cloud Infrastructure (OCI). Na OCI, são armazenados e processados a maior parte dos dados da Engelmig, sendo, assim, o principal conjunto de recursos críticos físicos da empresa.

2.4. INFRAESTRUTURA DE REDE

Equipamentos de rede, como roteadores, switches e firewalls, que são necessários para garantir a conectividade e segurança dos sistemas de informação da empresa.

2.5. SISTEMAS DE CONTROLE DE ACESSO

Os sistemas de controle de acesso, como senhas, autenticação multifator e sistemas de gerenciamento de identidade, são essenciais para garantir a segurança dos sistemas de informação da empresa.

A Engelmig utiliza o Active Directory (AD) do Sistema Operacional Windows como sua aplicação principal de segurança de acessos. Esta aplicação é executada em um servidor e autoriza todos os logins dos usuários

do Sistema Operacional em qualquer unidade da Engelmig, permitindo o acesso ao Windows nas estações de trabalho dos usuários.

Além do Active Directory, a Engelmig também utiliza sistemas de controle de acesso incorporados aos próprios ERPs, como ZEUS, SENIOR e a Intranet. Nesses sistemas, um usuário administrador tem a responsabilidade de liberar ou revogar acessos, que podem ser específicos para uma aplicação, uma tela ou até mesmo um determinado campo. Para facilitar o processo de gestão de acessos, esses sistemas oferecem a funcionalidade de copiar as permissões de um usuário para outro.

Esses controles de acesso são fundamentais para manter a integridade, confidencialidade e disponibilidade das informações, garantindo que apenas usuários autorizados possam acessar e manipular dados críticos da organização.

2.6. EQUIPE DE TI

A Equipe de Tecnologia da Informação (TI) é responsável por garantir que todos os processos de geração, utilização e compartilhamento de informações da empresa funcionem de maneira eficiente e segura.

Os profissionais de TI da Engelmig são capacitados e especializados em diversas áreas de Tecnologia da Informação. Eles atuam em diferentes níveis de suporte, incluindo:

- **Suporte Nível 1:** Encarregado de atender diretamente os usuários, resolvendo problemas imediatos e fornecendo assistência técnica básica.
- **Suporte Nível 2:** Focado na análise de dados, gestão de sistemas e resolução de problemas mais complexos que não puderam ser resolvidos pelo Suporte Nível 1.
- **Suporte Nível 3:** Escalonado para a empresa terceirizada Prolinx, que possui um time de especialistas em diversos temas. Este nível também é escalonado para os fornecedores dos ERPs, como Atlanta Sistemas ou Senior, para tratar de questões específicas e avançadas relacionadas aos sistemas.

Esses profissionais trabalham em conjunto para assegurar a continuidade dos serviços de TI, implementar novas tecnologias, manter a infraestrutura segura e eficiente, e garantir que todos os sistemas de informação da empresa estejam operando de acordo com as melhores práticas e políticas de segurança estabelecidas.

Quaisquer demandas ao TI deverão ser solicitadas via chamado no e-mail suporte@engelmig.com.br ou por telefone/WhatsApp (33) 3339-3837.

3. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

É o que trata este documento. São as políticas, procedimentos e controles que estabelecem a estrutura de segurança da informação da empresa, que são essenciais para garantir a conformidade regulatória e a segurança dos sistemas de informação.

3.1. COMPOSIÇÃO DA EQUIPE RESPONSÁVEL

É necessário definir uma Equipe ou Comitê responsável pelo desenvolvimento dos procedimentos, instruções e demais informações contidas na Política de Segurança da Informação.

É recomendado que colaboradores de outros de departamentos além do TI estejam presentes no Comitê, de forma a engajar outras áreas na Gestão da Política. Neste documento, muito se fala sobre compliance, regulamentação, ética, organização e outros tópicos que podem e devem ter a participação do Jurídico, RH e até mesmo da Diretoria.

A ENGELMIG possui um Comitê de Inovação e Tecnologia (COIT) com representantes de diversas áreas, porém este grupo tem caráter executivo e é convocado para deliberar projetos de grande impacto. Seria prudente a criação de outro Comitê como foi escrito no parágrafo acima para implementar e acompanhar a Política de Segurança da Informação na empresa.

3.2. COMITÊ DE INOVAÇÃO E TECNOLOGIA

A Engelmig constituiu um Comitê de Inovação e Tecnologia (CIT) com o objetivo de discutir e implementar melhorias contínuas em áreas críticas, como Segurança da Informação, Treinamentos, Investimentos em Tecnologias e ações de prevenção de perda de dados. Este comitê aborda temas específicos, incluindo:

- **Segurança da Informação:** Desenvolvimento e aprimoramento de estratégias para proteger as informações da empresa.
- **Treinamentos:** Programas de capacitação contínua para os funcionários, visando a adoção de boas práticas de segurança.
- **Investimentos em Ferramentas de Proteção:** Avaliação e implementação de soluções robustas para proteção contra ameaças.
- **Monitoramento de Invasões e Análises de Vulnerabilidade:** Procedimentos para detecção e resposta a tentativas de invasão, incluindo testes de penetração (Pentest).
- **Compliance:** Garantia de conformidade com as regulamentações e diretrizes estabelecidas pelos órgãos competentes.

As responsabilidades do Comitê incluem:

- **Objetivo do Comitê:** Estabelecer diretrizes e coordenar esforços para melhorar a segurança e a eficiência tecnológica da empresa.

- **Escopo dos Trabalhos:** Definir e priorizar as atividades a serem realizadas, incluindo a implementação de novas tecnologias e processos.
- **Definição dos Papéis e Responsabilidades:** Especificar as funções de cada membro do comitê, garantindo clareza e eficiência na execução das tarefas.

O Comitê de Inovação e Tecnologia desempenha um papel vital na promoção de uma cultura de segurança e inovação contínua, assegurando que a Engelmig esteja sempre alinhada com as melhores práticas e normas do mercado.

3.3. IMPLEMTNAÇÃO DA POLÍTICA

Este documento inteiro poderá ser compartilhado com toda a empresa, mas devido ao seu tamanho extenso, dificilmente será lido na íntegra pelos funcionários. Assim, é prudente segmentar a informação, “quebrando” em pedaços menores para envios periódicos.

Os meios de divulgação e periodicidade já deverão ter sido definidos na primeira reunião ordinária. Para facilitar a absorção do conhecimento pelos diversos colaboradores da empresa, é recomendado envios semanais ou quinzenais com textos mais curtos e utilização de recursos gráficos, de forma semelhante às “Pílulas” que o Departamento de RH vem divulgando há algum tempo.

Desta forma, procura-se alcançar também aqueles que tem menos conhecimento técnico dos assuntos tecnológicos, otimizando o alcance dos itens da Política. Tópicos mais complexos abordados neste documento seriam divulgados e discutidos somente em grupos com conhecimento mais técnico.

Todo novo colaborador deverá receber o material completo, assim como todas as pílulas já enviadas previamente à sua contratação.

3.4. ACOMPANHAMENTO E ATUALIZAÇÃO

É necessário acompanhar a divulgação da Política, buscando eventualmente pesquisar junto aos colaboradores sobre o conhecimento adquirido por eles. Pode-se utilizar formulários de pesquisa, ou mesmo enviar e-mails e/ou mensagens via whatsapp para questionar sobre determinados itens. Estas pesquisas podem ser semestrais.

A Política deverá passar por revisões programadas pelo menos duas vezes ao ano, ou caso tenha alguma mudança de processo em qualquer assunto abordado neste texto.

APROVAÇÃO	AUTORIZAÇÃO	
NOME/CARGO:	NOME/CARGO:	DATA:
ERICH CARLOS DE OLIVEIRA LÍDER CORPORATIVO DE SUPORTE	JULIANO ALEXANDRE CHANDRETTI GESTOR CORPORATIVO DE SUPORTE	29/05/2024