Política de segurança da Informação

Ela tem como objetivo estabelecer diretrizes para resguardar as informações da Bruning, assegurando proteção adequada durante todo o ciclo de vida da informação. A política está ligada diretamente a:

- TI (Tecnologia da Informação)
- SGSI (Sistema de Gestão de Segurança da Informação)
- LGPD (Lei Geral de Proteção de Dados)

A política inclui diretrizes para proteger ativos de informação físicos e lógicos, garantindo sua disponibilidade, assegurando que a informação esteja acessível quando necessário; integridade, garantindo a preservação, consistência e confiabilidade das informações e sistemas; e confidencialidade, para proteger as informações contra a divulgação não autorizada.

As diretrizes devem ser seguidas por todos os colaboradores, terceiros e demais pessoas que trabalham para a Bruning Tecnometal. A política informa que os ambientes, sistemas, computadores, rede e dispositivos da empresa podem ser monitorados e gravados conforme as leis brasileiras.

O uso inadequado das informações, equipamentos e ferramentas de comunicação pode resultar em sanções administrativas, civis e/ou criminais, conforme as disposições da LGPD e das leis trabalhistas vigentes.

Classificação da Informação

- Informação Confidencial: Deve ser mantida em sigilo absoluto para evitar perdas financeiras, danos à imagem ou perda de competitividade. Usa exposição fora da organização pode causar sérios prejuízos.
- Informação Restrita: Limitada a um grupo específico de usuários responsáveis pela sua produção ou tratamento. Compartilhada internamente e, quando necessário, externamente. Possui um nível médio de confidencialidade.
- Informação Interna: Desatinada ao conhecimento interno da organização. Caso seja divulgada, o impacto não será significativo para a empresa.
- Informação Pública: Pode ser divulgada a todos, incluindo funcionários, terceirizados, clientes, fornecedores e público em geral, sem causar impactos negativos ao negócio.

Mas o SGSI se direciona a quais pessoas?

A alta direção se compromete a garantir que os processos e recursos necessários para a manufatura dos produtos e o processamento das informações sejam implementados, mantidos e monitorados, nomeando o responsável pela área de Tecnologia e Segurança da Informação como responsável pelo SGSI.

Vale destacar que é responsabilidade de todos e todas seguir as diretrizes e regras propostas na política e incentivar os demais a fazer o mesmo, pois a segurança da informação é dever de cada pessoa que faz parte do processo.

As Responsabilidades com a Segurança da Informação ficam distribuídas da seguinte forma:

- Alta Direção: Prover recursos para a implementação e melhoria da segurança da informação.
- Comitê de Segurança da Informação: Discutir e aprovar regras propostas, definir e aprovar o orçamento para segurança e infraestrutura.
- Equipe de Tecnologia e Segurança da Informação: Implementar, manter e monitorar o SGSI, propor ajustes e modificações na estrutura normativa.
- Gestão e Lideranças de Todas as Áreas: Apoiar e assegurar o cumprimento das políticas de segurança.
- Recursos Humanos: Seguir procedimentos durante seleção, admissão, transferência e demissão de colaboradores.
- Jurídico: Manter áreas informadas sobre alterações legais e regulatórias.
- Todos os Usuários: Zelar pela proteção das informações e seguir as regras estabelecidas na política.

Requisitos Gerais de Segurança da Informação:

- Segurança do Ambiente Tecnológico: Equipamentos e ativos de informações devem estar em áreas fisicamente seguras com controle de acesso adequado.
- Ativos Tecnológicos: Os ativos de suporte fornecidos pela Bruning Tecnometal devem ser usados corretamente e protegidos.
- Privacidade e Proteção de Dados: Manter o sigilo e a confidencialidade dos dados, evitando transmissões não autorizadas.
- Comportamento em Ambientes de TI: Usar ferramentas de TI com responsabilidade, sem acessar ou compartilhar informações ofensivas ou falsas.
- Mesa e Tela Limpa: Informações críticas devem ser armazenadas em locais seguros quando não estiverem em uso.
- Propriedade Intelectual: Respeitar os direitos autorais e de cópia de imagens, textos, softwares, entre outros.
- Informação Sensível: Informações confidenciais não devem ser reveladas sem autorização prévia.
- Dados Pessoais: Seguir as regras para tratar informações pessoais, incluindo proteção e descarte adequados.
- Dispositivos Móveis e Trabalho Remoto: Implementar mecanismos de proteção como certificados digitais, VPN, antivírus e criptografia.
- Celulares, Scanners e Tecnologia de Gravação de Áudio e Vídeo: Evitar o uso desses dispositivos em áreas com informações confidenciais, a menos que necessário.

Conceitos e definições fundamentais nesse processo.

- Ativo: Qualquer elemento que agregue valor ao negócio, podendo ser uma informação digital ou física, hardware, software, pessoa ou ambiente físico.
- Ativo de Informação: Informações essenciais para o negócio que precisam ser protegidas.
- Ativos de Suporte: Recursos associados à informação e ao processamento da informação, como hardware, software, sistemas de TI e funcionários.
- Segurança da Informação: Proteção dos ativos da organização contra diversas ameaças.
- Sistema da Informação: Sistema pelo qual são obtidos dados para as operações de controle e planejamento da empresa.
- Incidente de Segurança da Informação: Evento ou conjunto de eventos que impactam a disponibilidade, integridade ou confidencialidade de um ativo de informação.

Você é responsável pelo cumprimento desta política.
Nos ajude a disseminar a informação e compartilhar este conhecimento com todas as pessoas da Bruning.

BRUNING TECNOMETAL