## 1. OBJETIVO

Estabelecer diretrizes e padrões internos que devem ser seguidos com o intuito de garantir a segurança da informação e a privacidades de dados da Metalkraft e das partes interessadas conforme definido no manual MN 01 em todas as relações.

## 2. APLICAÇÃO E RESPONSABILIDADE

Aplica-se a todos as partes interessadas com acesso à informação da Metalkraft, em qualquer formato (físico, digital, visual ou verbal), em todas as fases do ciclo de vida (criação, armazenamento, processamento, transmissão e descarte), incluindo também todos os ambientes físicos, tecnológicos e recursos disponibilizados pela Metalkraft.

| | |
|---|---|
| Responsabilidades Gerais | •Cumprir a Política e seus procedimentos<br>•Proteger informações, sistemas e equipamentos.<br>•Manter sigilo sobre dos dados.<br>•Adotar comportamento seguro com dados, redes e ativos de informação.<br>•Relatar ameaças, incidentes ou suspeitas imediatamente. |
| Alta Direção | •Garantir recursos e apoio.<br>•Promover a cultura de segurança da informação e privacidade dos dados.<br>•Aprovar Política da Segurança da Informação |
| Tecnologia da Informação | •Implementar, monitorar e revisar controles de segurança da informação, incluindo procedimentos de bloqueio, restrições no sistema operacional e uso de certificados digitais.<br>•Gerenciar acessos, infraestrutura, backups, auditorias e trilhas de evidência, garantindo bloqueios imediatos em casos de desligamento ou incidente.<br>•Controlar dispositivos e conexões, impedindo o uso de equipamentos não autorizados e assegurando atualizações permanentes das proteções contra ameaças.<br>•Conduzir análises de risco, monitoramento contínuo do ambiente, ações preventivas e planos de continuidade. |
| Gestão de Pessoas | •Conduzir treinamentos e conscientização.<br>•Desenvolver a cultura da segurança da informação e privacidades dos dados.<br>•Levantar os Requisitos Legais na esfera jurídica.<br>•Gerenciar desvios e infrações dessa Política na esfera de jurídica trabalhista. |
| Patrimônio | •Controlar acessos físicos/predial |
| Compras | •Avaliar riscos de terceiros |
| Sistema de Gestão | •Manter os documentos atualizados no sistema integrado de gestão. |
| Comitê de Segurança da Informação e Privacidade dos Dados | •Garantir a conformidade e proteção de dados pessoais, corporativos e estratégicos da organização, mantendo o sigilo e confidencialidade.<br>•Gestão de incidentes<br>•Consequência de não conformidade<br>•Revisão da Política da Segurança da Informação |

## 3. DEFINIÇÕES E ABREVIAÇÕES

**Ativos de informação:** Refere-se a um conjunto de conhecimento organizado e gerenciado como uma entidade única. Como qualquer outro recurso corporativo, eles possuem valor financeiro, que aumenta em relação direta com o número de pessoas que são capazes de usar as informações. De forma geral, tudo o que para uma empresa for uma informação que tenha relação com o funcionamento no dia a dia, passa a ser um ativo com importância a ser protegido.

**Confidencialidade:** Refere-se a garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

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

**Integridade:** Refere-se 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.

**KPI**: Key Performance Indicator - Indicadores de desempenho

**LGPD**: Lei Geral de Proteção de Dados

**SLA:** Service Level Agreement - Acordo de Nível de Serviço

**SDLC**: Software development life cicle - Ciclo de vida de Desenvolvimento de Software

**TI:** Tecnologia da Informação

**VPN**: Virtual Private Network - Rede Privada Virtual

## 4. DESCRIÇÃO DAS ATIVIDADES

### 4.1. Introdução

Para a Metalkraft, a informação é um ativo valioso e qualquer forma ou meio de comunicação deve ser compartilhada, armazenada com responsabilidade devendo ser tratada com responsabilidade e protegida de forma adequada. Essa proteção deve ser sempre proporcional ao risco ao qual as informações estão expostas. A segurança da informação é guiada pelos seguintes aspectos essenciais:

- Confidencialidade: acesso apenas a pessoas autorizadas.
- Integridade: informações corretas, íntegras e controladas.
- Disponibilidade: disponibilidade e rápida recuperação de sistemas e dados conforme necessidade.

A Metalkraft tem o compromisso de proteger as informações das partes interessadas em todas as suas relações de negócio que lhe são confiadas, gerenciando os riscos e atendendo as legislações vigentes.

### 4.2. Estratégia de gestão de riscos de informação

O gerenciamento de riscos deve orientar a estratégia de segurança da informação. Ele deve determinar as ações e prioridades de gerenciamento para proteger contra os riscos de segurança da informação identificados. A metodologia de gestão de risco é baseada em:

O gerenciamento de riscos deve orientar a estratégia de segurança da informação. Ele deve determinar as ações e prioridades de gerenciamento para proteger contra os riscos de segurança da informação identificados. A metodologia de gestão de risco é baseada conforme descrito no P 03 - Análise de risco e oportunidade e no FOR-095 - Matriz de gerenciamento risco e oportunidade da TI.

### 4.3. Avaliação dos riscos

No FOR-095 é levado em consideração as ocorrências e os efeitos abaixo:

As ocorrências podem ser:

- Acidentais (falhas humanas, desastres físicos ou naturais, etc.).
- Internas maliciosas (fraudes, desvio de conduta, abuso de acesso, etc.).
- Externas maliciosas (ataques cibernéticos, phishing, invasão de hackers, etc.).
- Fragilidade em pessoas (esquecimento de senha exposta em papel; clicar em link de phishing; erro ao enviar arquivo confidencial para destinatário incorreto).
- Fragilidade em processos (ausência de dupla checagem em processos críticos; falta de revisão de acessos; procedimentos desatualizados).
- Fragilidade em sistemas (softwares sem atualização; senhas fracas; sistemas sem antivírus; portas de rede abertas sem necessidade).
- Infraestrutura vulnerável (salas sem controle de acesso; equipamentos sem backup; cabos expostos).

Os efeitos podem ser:

- Danos pessoais.
- Perdas financeiras.
- Consequências legais.
- Interrupção ou dificuldade na continuidade do negócio.
- Perda da confiança do cliente.
- Redução da competitividade.
- Prejuízo à reputação da empresa.

### 4.4. Gestão de ativos

A gestão de ativos garante que todos os recursos de informação e TI da Metalkraft sejam identificados, inventariados periodicamente e protegidos. Cada ativo possui um responsável por sua segurança e uso adequado. Os acessos são individuais e controlados pela TI, que também autoriza instalações, atualizações e monitora o ambiente. Equipamentos e informações só podem ser utilizados por pessoas autorizadas, seguindo classificação e regras de proteção definidas. As informações confidenciais só devem ser divulgadas para pessoas autorizadas com base na “necessidade do saber” e com o compromisso assinado para o tratamento adequados dos dados (termos / aditivos de contratos) em consonância com os procedimentos internas.

A Metalkraft estabelece controles e medidas internas adequadas para garantir a segurança da informação em todo o processo do contrato do funcionário e terceiros na organização independente do status do contrato (da admissão à demissão).

### 4.5. Propriedades de ativos

As informações pertencem à empresa, independentemente de onde estejam armazenadas. Cada ativo deve ter um responsável por avaliar riscos, definir proteções e garantir sua segurança física e lógica, além de responder por incidentes relacionados ao ativo.

### 4.6. Classificação de ativo

Todos os ativos devem ter um responsável por definir nível de proteção e garantir segurança física e lógica.

| Serviço de Segurança | Classe |
|---|---|
| Confidencialidade | Pública |
| | Interna |
| | Confidencial |
| Integridade | Normal |
| | Importante |
| | Altamente Importante |
| Disponibilidade | Normal |
| | Espelhada |
| | Altamente Disponível |
| | Sites Duplos |

### 4.7. Segurança Física

A segurança física visa proteger instalações e ativos de informação contra acessos não autorizados, danos ou perdas, por meio de controles que garantem a proteção dos ambientes e o acesso apenas a pessoas autorizadas.

- Acessos às instalações são controlados.
- Monitoramento por câmeras.
- Áreas críticas com acesso restrito.
- Equipamentos e documentos protegidos.
- Impressoras e materiais confidenciais mantidos em áreas controladas.
- Visitantes devem estar acompanhados.

### 4.8. Gestão de Operação de TI

As operações de TI devem seguir boas práticas, com documentação formal, segregação de funções e controle de mudanças. Ambientes de desenvolvimento, teste e produção devem ser separados, e fornecedores de TI gerenciados por SLAs e KPIs. Sistemas devem possuir antivírus atualizado, controles de código móvel confiável e backups protegidos e testados. Todo acesso à internet deve passar pelos firewalls da Metalkraft, e qualquer publicação ou coleta de dados deve seguir aprovação formal e atender a LGPD.

#### *4.8.1. E-mail corporativo e Internet*

- Todo tráfego é monitorado.
- Utilização restrita a atividades profissionais.
- Instalações só podem ser realizados mediante liberação da TI.
- É proibido enviar dados ou documentos da empresa sem autorização.

#### *4.8.2. Uso do VPN (Virtual Private Network) ou Rede Privado*

Os funcionários da empresa assinam um termo de ciência no momento da contratação, comprometendo-se a utilizar o VPN de forma consciente, segura e responsável. Ao fazer isso, garantem a segurança dos dados e a integridade das informações acessadas, zelando pelo bom uso dos equipamentos fornecidos pela empresa.

### 4.9. Desenvolvimento, Aquisição e Manutenção de Sistemas

Os sistemas de informação devem incorporar requisitos de segurança desde a especificação e o design, garantindo menor custo e maior eficiência ao longo do ciclo de vida. A aquisição e o desenvolvimento devem seguir processos formais que identifiquem controles proporcionais aos riscos. O processamento das aplicações deve assegurar a integridade e validade das informações.

Alterações em sistemas operacionais precisam ser validadas para evitar conflitos, e qualquer desenvolvimento terceirizado deve seguir um SDLC - Ciclo de vida de Desenvolvimento de Software supervisionado com testes de segurança. Deve existir um processo estruturado para monitorar vulnerabilidades, aplicar patches e atualizar sistemas. Sistemas operacionais e softwares padrão devem ser reforçados, com remoção de serviços desnecessários e revisão dos parâmetros de segurança sendo responsabilidade da TI.

### 4.10. Gestão de incidentes

Todos os incidentes devem ser reportados em um dos canais abaixo, não é permitido realizar contra-ataque:

- comitê da segurança da informação e privacidade dos dados
- liderança
- Tecnologia da Informação
- e-mail: lgpd@metalkraft.com.br

### 4.11. Continuidade de negócios

A Metalkraft mantém um Plano de Contingência para assegurar resposta adequada, continuidade das operações e recuperação rápida em situações críticas.

- Plano de contingência documentado e revisado periodicamente;
- Continuidade assegurada em casos de falha tecnológica, desastres naturais, perda de acesso ou outras interrupções.
- Processos críticos mapeados e com planos de recuperação.

### 4.12. Conformidade

- Atender LGPD, normas ISO, TISAX e requisitos contratuais.
- Utilizar apenas softwares licenciados.
- Registros protegidos e armazenados conforme tempo legal.
- Requisitos legais vigentes.

### 4.13. Violação da Política da Segurança da Informação

Qualquer violação desta Política será analisada e tratada pelo Comitê de Segurança da Informação e Privacidade dos Dados e poderá resultar em medidas disciplinares em conformidade com as legislações pertinentes e com o nosso Código de Conduta.

- Violações leves: advertência verbal;
- Violações moderadas: advertência escrita;
- Violações graves: suspensão disciplinar ao trabalho até demissão por justa causa.

Ser responsabilizado legalmente. Penalidade na legislação brasileira (trabalhista, civil e penal).

### 4.14. Revisão e Melhoria da Política

A Metalkraft através do comitê tem o compromisso de revisar e melhorar esta Política de Segurança da Informação, bem como, seus processos e medidas internas de controle de acordo com a necessidade. Portanto, o comitê tem liberalidade para propor alterações para a Alta Direção da organização.

## 5. DOCUMENTOS RELACIONADOS

- ABNT NBR ISO/IEC 27001
- ABNT NBR ISO/IEC 27002
- LGPD Lei nº 13.709, de 14 de agosto de 2018
- TISAX VDA 5.1
- Código De Conduta Interno
- Termo de Ciência, Autorização e Consentimento do Titular para Coleta e Tratamento de Dados Pessoais
- Termo de Responsabilidade do Operador para Tratamento dos Dados Pessoais
- Contrato de Trabalho – Termo de Confidencialidade e Sigilo
- Termo do Visitante
- Termo de Sigilo e Compromisso Comitê
- MN 001 - Manual do Sistema Integrado de Gestão
- P 03 - Análise de risco e oportunidade
- P 08 - Conscientização e Motivação
- FOR-095 - Matriz de gerenciamento de risco e oportunidade

## 6. ALTERAÇÃO E APROVAÇÃO

| Revisão | Data | Elaborador | Aprovador | Resumo da alteração |
|---|---|---|---|---|
| 00 | 12/12/2025 | Robson Ferreira de Oliveira<br>Luciane Vilas Boas<br>André Baldessar | Thiago Stahlke | Emissão inicial |