Sumário

1. Objetivo....2
2. Escopo....2
3. Requisitos de Segurança para Fornecedores....2
   3.1. Certificação de Segurança da Informação....2
   3.2. Classificação e Gestão de Fornecedores....2
   3.3. Cláusulas Contratuais....3
   3.4. Confidencialidade....3
   3.5. Monitoramento e Auditoria....4
   3.6. Proteção de Dados e Transferência de Informações....4
   3.7. Fornecedores que tenham acesso a sistemas, redes ou dados confidenciais da Metaltork deverão comprovar:....5
   3.8. Segurança em Serviços Compartilhados (Multi-Tenant)....5
5. Penalidades e Consequências....5
6. Atualização....5
7. Revisão:....5

1. Objetivo

Esta política estabelece os requisitos mínimos de segurança da informação para fornecedores, prestadores de serviços e parceiros da Metaltork. O objetivo é garantir a proteção das informações corporativas, reduzir riscos operacionais e manter conformidade com normas e regulamentações aplicáveis, incluindo TISAX e ISO 27001.

2. Escopo

Esta política se aplica a todos os fornecedores que prestam serviços ou fornecem produtos que envolvem o processamento, armazenamento ou transmissão de informações da Metaltork, independentemente de sua localização geográfica ou forma de contratação.

3. Requisitos de Segurança para Fornecedores

3.1. Certificação de Segurança da Informação

Fornecedores de serviços de TI devem possuir certificação de segurança da informação reconhecida, como TISAX, ISO 27001 ou equivalente.

Caso não possuam certificação, os fornecedores deverão preencher o Checklist de Segurança da Informação da Metaltork e serem aprovados antes da contratação, conforme critérios abaixo:

Pontuação abaixo de 59% do checklist → Reprovado. O fornecedor não poderá prestar serviços à Metaltork, salvo em casos excepcionais mediante derroga aprovada pela Gestão de Segurança da Informação.

Pontuação entre 60% e 75% do checklist → Aprovado Condicionalmente. O fornecedor poderá ser contratado desde que apresente um Plano de Ação de Melhorias, com prazos definidos e acompanhamento periódico.

Pontuação superior a 75% do checklist → Aprovado. O fornecedor atende aos requisitos mínimos e pode ser contratado sem restrições adicionais.

3.2. Classificação e Gestão de Fornecedores

Todos os fornecedores serão classificados de acordo com o nível de criticidade dos serviços prestados e o nível de confidencialidade das informações acessadas:

Alto risco: acesso a informações estratégicas e críticas.

Médio risco: acesso a dados internos e operacionais.

Baixo risco: sem acesso direto a informações sensíveis.

Fornecedores de alto e médio risco estarão sujeitos a auditorias periódicas e processos de requalificação anuais.

3.3. Cláusulas Contratuais

Todos os contratos devem conter cláusulas que garantam a conformidade com esta política e exigências regulatórias aplicáveis.

Os contratos devem especificar:

Requisitos de proteção e manuseio das informações.

Procedimentos para exclusão e devolução segura de dados em caso de término de contrato.

Requisitos para subcontratados, que também deverão aderir a esta política.

Adicionalmente, os contratos com fornecedores de TI deverão incluir uma cláusula específica sobre o Término de Serviços e Remoção Segura de Ativos de Informação", que obrigatoriamente detalhará:

O método de exclusão segura a ser utilizado pelo fornecedor para apagar todos os dados da Metaltork de seus ambientes, incluindo cópias de segurança. A destruição física ou a sanitização de mídias (sobrescrita de dados) são exemplos de métodos aceitáveis.

A emissão de um "Certificado de Remoção Segura" pelo fornecedor ao final do processo, que servirá como evidência formal do cumprimento da obrigação. Este certificado deverá ser anexado ao chamado de encerramento de contrato no sistema GLPI.

O direito da Metaltork de auditar o processo de remoção segura, caso julgue necessário, especialmente para fornecedores de alto risco.

3.4. Confidencialidade

A proteção das informações da Metaltork é mandatória em todas as frentes de relacionamento com fornecedores, desde a prospecção inicial até o completo encerramento do vínculo contratual. As obrigações de confidencialidade são aplicadas em duas fases distintas e complementares:

Fase de Prospecção e Cotação (Pré-Contratual)

Antes do compartilhamento de qualquer informação classificada como "Sensível" ou "Confidencial" para fins de cotação, é obrigatória a assinatura do NDA pelo fornecedor em prospecção. Nenhum desenho técnico, especificação ou dado de protótipo será compartilhado sem que o referido termo esteja devidamente assinado e arquivado pela área responsável (Compras/Comercial).

Fase Contratual (Pós-Aceite do Pedido de Compra)

Uma vez estabelecida a relação comercial, o fornecedor reconhece e concorda que, ao aceitar o Pedido de Compras emitido pela Metaltork, estabelece-se uma relação contratual vinculada às condições gerais descritas no referido documento. Este ato reforça o compromisso com a confidencialidade das informações trocadas, já formalizado pelo Termo de Confidencialidade assinado previamente.

Consideram-se informações confidenciais todos os dados, documentos, comunicações, especificações técnicas, projetos, desenhos, instruções, metodologias, estratégias e quaisquer outros materiais fornecidos pela Metaltork durante ou em decorrência da relação comercial, independentemente da forma de transmissão (escrita, oral, eletrônica ou física).

Esta obrigação de sigilo estende-se aos colaboradores, subcontratados e representantes do fornecedor, e permanecerá vigente mesmo após o encerramento do vínculo comercial, salvo se houver autorização expressa da Metaltork em sentido contrário.

A assinatura de um Termo de Confidencialidade (NDA) adicional poderá ser requerida em casos específicos que envolvam acesso contínuo a informações estratégicas, dados sensíveis ou ambientes críticos da empresa.

O acesso de fornecedores aos sistemas e redes da Metaltork será concedido somente mediante aprovação formal e conforme o princípio do menor privilégio.

Contas de acesso devem ser individuais, registradas e monitoradas.

3.5. Monitoramento e Auditoria

A Metaltork realizará auditorias periódicas para avaliar a conformidade dos fornecedores com esta política.

Fornecedores críticos devem fornecer relatórios periódicos de segurança, incluindo indicadores de desempenho (KPIs) e cumprimento de Acordos de Nível de Serviço (SLAs).

Incidentes de segurança devem ser reportados imediatamente à Metaltork.

3.6. Proteção de Dados e Transferência de Informações

A transferência de informações deve ser realizada de forma segura e rastreável.

Caso o projeto seja classificado como confidencial, os dados devem ser transferidos exclusivamente por canais seguros e criptografados.

A homologação de ferramentas de transferência de arquivos deve ser feita previamente, priorizando soluções seguras como OneDrive ou outras plataformas corporativas aprovadas.

Fornecedores devem garantir que seus funcionários sejam treinados e conscientizados sobre boas práticas de segurança da informação.

3.7. Fornecedores que tenham acesso a sistemas, redes ou dados confidenciais da Metaltork deverão comprovar:

- Uso de antivírus corporativo atualizado;
- Aplicação de atualizações de segurança em seus dispositivos;
- Política de backup e resposta a incidentes documentada;
- Procedimento de reporte imediato em caso de incidentes que envolvam dados da Metaltork;

3.8. Segurança em Serviços Compartilhados (Multi-Tenant)

- Fornecedores que oferecem serviços em uma infraestrutura compartilhada (ex: Software como Serviço - SaaS, plataformas em nuvem) devem, obrigatoriamente, fornecer documentação que descreva seu conceito de segregação de clientes.
- O conceito de segregação deve detalhar, no mínimo, os controles implementados para a separação lógica de dados, funções, redes, sistemas operacionais e sistemas de armazenamento entre os diferentes clientes.
- A avaliação e aprovação deste conceito são mandatórias antes da contratação e serão revalidadas periodicamente, conforme o nível de risco do fornecedor, para garantir a proteção contínua das informações da Metaltork."

5. Penalidades e Consequências

O descumprimento desta política poderá resultar em:

Advertências formais e exigência de ações corretivas.

Revisão e possível suspensão do contrato de fornecimento.

Ações legais em casos de negligência grave ou vazamento de informações.

6. Atualização

Esta política será revisada anualmente ou conforme necessário para refletir mudanças nas exigências regulatórias, melhores práticas de segurança da informação e requisitos da Metaltork.

7. Revisão:

00 – Revisão inicial.

01 – Ajustes para tratativa de NC auditoria interna Tisax. 07/07/2025

Elaborado por:	Aprovador:
Gabriel Amaral – Supervisor de TI	Charles Anderle – Gerente de TI