POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA FORNECEDORES ARCELORMITTAL GONVARRI

Esta política tem como objetivo estabelecer diretrizes e expectativas claras de segurança da informação para proteger os ativos da empresa ARCELORMITTAL GONVARRI em suas interações com fornecedores. A segurança da informação é essencial para assegurar a confidencialidade, integridade e disponibilidade das informações, garantir conformidade com as regulamentações legais, preservar a reputação e a confiança dos clientes, e manter a continuidade das operações de negócios.

2. Termos e Definições

LGPD: Lei Geral de Proteção de Dados Pessoais
SI: Segurança da Informação
Ativo: Algo que tem valor para a organização e deve ser protegido.
Políticas de Segurança da Informação: Conjunto de diretrizes, regras e práticas para proteger a confidencialidade, integridade e disponibilidade das informações.
TISAX: Trusted Information Security Assessment Exchange, um padrão de segurança para a indústria automotiva.

3. Confidencialidade dos Dados

Os fornecedores devem reconhecer que todas as informações e dados fornecidos pela ARCELORMITTAL GONVARRI são confidenciais e devem ser tratados de forma segura.
Medidas adequadas devem ser implementadas pelos fornecedores para proteger os dados contra acesso não autorizado, uso indevido ou divulgação.
É proibida a divulgação de informações a terceiros sem autorização por escrito da ARCELORMITTAL GONVARRI.
Os fornecedores devem adotar políticas de não revelação e acordos de proteção de dados.

4. Segurança na Relação com Fornecedores

4.1 Política de Segurança da Informação nas Relações com Fornecedores

Uma avaliação de segurança deve fazer parte do processo de homologação de fornecedores, conforme estabelecido nas políticas de gestão de terceiros.
Os controles de segurança devem cobrir processos e procedimentos que a ARCELORMITTAL GONVARRI e os fornecedores devem implementar.
Tipos de acesso à informação por fornecedores devem ser definidos, supervisionados e controlados.
Requisitos mínimos de segurança devem ser especificados para cada tipo de informação e acesso, servindo de base para acordos contratuais.
Processos e procedimentos devem ser implementados para monitorar o cumprimento dos requisitos de segurança por parte dos fornecedores.

Deve haver obrigações claras para garantir a integridade e a exatidão das informações tratadas por qualquer uma das partes.
Os fornecedores devem atender às condições de gestão de incidentes relacionadas ao acesso e devem ser responsáveis por qualquer falha.
Devem ser estabelecidos acordos de resiliência, recuperação e contingência para garantir a continuidade das operações.
A segurança durante a migração de dados, infraestrutura de TI e instalações de tratamento deve ser garantida.

4.2 Requisitos de Segurança da Informação em Contratos com Terceiros

Todos os riscos e requisitos de segurança relevantes devem ser incluídos em contratos, contemplando subcontratados, quando necessário.
Procedimentos de continuidade dos serviços devem ser previstos para casos de impossibilidade de fornecimento.
Deve haver cláusulas obrigatórias de confidencialidade e privacidade de dados, revisadas periodicamente.
Os contratos devem definir o acesso permitido, os métodos de transmissão de dados e a classificação da informação.
Os contratos devem incluir políticas de uso aceitável e listas do pessoal autorizado a acessar informações da ARCELORMITTAL GONVARRI.
Devem constar políticas de gestão de incidentes, treinamentos, regras de subcontratação e auditorias.
É responsabilidade do fornecedor garantir que subcontratados cumpram os requisitos de segurança da ARCELORMITTAL GONVARRI.
Procedimentos de eliminação segura de dados devem ser seguidos, documentados e comprovados.

4.3 Cadeia de Suprimentos de Tecnologia da Informação e Comunicações

Os contratos devem abordar riscos de segurança da cadeia de suprimentos de TI e comunicações.
A ARCELORMITTAL GONVARRI deve trabalhar com fornecedores para entender e garantir a segurança em todas as etapas da cadeia de suprimentos.
Deve haver requisitos de segurança que se estendam por toda a cadeia, com processos de supervisão e validação.
Componentes críticos de produtos ou serviços devem ser rastreados e protegidos para garantir que não tenham funcionalidades indesejadas.
Regras para troca de informações e gestão de possíveis problemas devem ser definidas.

5. Disponibilidade dos Dados

É responsabilidade do fornecedor garantir a disponibilidade dos dados, minimizando interrupções e tempo de inatividade.
Devem existir procedimentos de backup e recuperação de dados para assegurar a continuidade dos serviços em caso de falhas ou desastres.
O fornecedor deve estabelecer acordos de resiliência, recuperação e contingência para

garantir a continuidade das operações.
Notificações imediatas à ARCELORMITTAL GONVARRI são obrigatórias em casos de interrupções nos serviços que possam afetar a disponibilidade dos dados.

6. Responsabilidades

A Direção de TI da ARCELORMITTAL GONVARRI é responsável por promover e apoiar o estabelecimento de medidas técnicas, organizacionais e de controle para garantir a autenticidade, integridade, disponibilidade, confidencialidade e auditabilidade das informações.
O Comitê de Segurança da Informação da ARCELORMITTAL GONVARRI deve gerenciar a política e revisar seu conteúdo periodicamente para garantir sua eficácia.
Os fornecedores devem cumprir todas as políticas de segurança da informação estabelecidas pela ARCELORMITTAL GONVARRI e nomear um representante responsável pela segurança da informação.
A ARCELORMITTAL GONVARRI deve comunicar suas políticas de segurança aos fornecedores e oferecer treinamento quando necessário.
O fornecedor é responsável por violações desta política e deve tomar medidas corretivas imediatas para remediar não conformidades.
O não cumprimento pode levar a medidas disciplinares, incluindo rescisão de contrato e responsabilidade legal.

7. Diretrizes e Requisitos para Fornecedores

Os fornecedores devem:
Respeitar as diretrizes e políticas de segurança da informação da ARCELORMITTAL GONVARRI.
Cumprir todas as leis, regulamentos e normas aplicáveis, incluindo a LGPD.
Submeter-se a análise de risco para identificar possíveis vulnerabilidades que possam impactar a segurança da informação.
Obter certificações de segurança da informação, como ISO 27001 ou TISAX, quando requisitado pela ARCELORMITTAL GONVARRI.
Formalizar o compromisso com a segurança da informação por meio de um contrato específico.
Utilizar as informações da ARCELORMITTAL GONVARRI apenas para os fins autorizados, mantendo um nível adequado de confidencialidade.
Garantir que a obrigação de manter a confidencialidade permaneça válida após o término do contrato.
Implementar controles de segurança robustos para evitar o uso indevido ou vazamento de dados.
Comunicar imediatamente à ARCELORMITTAL GONVARRI qualquer incidente de segurança, perda de dados ou possível violação de segurança.
Relatar todos os incidentes de segurança à equipe de segurança da informação da ARCELORMITTAL GONVARRI.
Garantir a eliminação segura de dados adquiridos após o término do contrato, conforme exigido pela legislação em vigor.
Permitir que a ARCELORMITTAL GONVARRI realize auditorias periódicas, incluindo visitas

às instalações do fornecedor para garantir a conformidade com as normas de segurança.

8. Documentação para Envio e Ciência

Política de segurança da informação: Compete ao departamento de compras enviar a Política de Segurança da Informação ao fornecedor. Para todos os fornecedores.
Revisão e Aceitação: O representante legal do fornecedor deve revisar a Política de Segurança da Informação e esclarecer eventuais dúvidas. Todos os requisitos referentes à Segurança da Informação que constam na política devem ser compreendidos e atendidos.

Contrato de Confidencialidade (NDA) e Privacidade de Dados: Obrigatória classe (A) Eventualmente aplicável classe (B) de Acesso a Informações Sensíveis
Distribuição do Contrato: Compete ao departamento de Compras fornecer uma cópia do Contrato de Confidencialidade para Fornecedores (NDA) e Privacidade de Dados ao representante legal do fornecedor.
Revisão e Aceitação: O representante legal do fornecedor deve revisar o Contrato de Confidencialidade, esclarecer eventuais dúvidas e assinar o documento para indicar aceitação dos termos.
Registro e Arquivamento: Uma cópia assinada do Contrato de Confidencialidade deve ser arquivada no departamento de Compras.
Medidas Corretivas: Caso seja identificado algum descumprimento do Contrato, serão aplicadas medidas corretivas, que podem incluir revisão do contrato, treinamento adicional ou rescisão do contrato, conforme a gravidade da violação.

Avaliação de Segurança da Informação e Privacidade de Dados (LGPD) Obrigatória classe (A) de Acesso a Informações Sensíveis:
Distribuição do formulário: fornecer o formulário "Avaliação de SI e LGPD" da ARCELORMITTAL GONVARRI ao representante legal do fornecedor.
Revisão e Aceitação: O representante legal do fornecedor deve revisar o formulário, esclarecer eventuais dúvidas, preencher e assinar o documento para verificar a aderência aos requisitos de Segurança da Informação e LGPD.
Registro e Arquivamento: Uma cópia assinada do formulário deve ser arquivada no departamento de Compras.
Não atendimento aos requisitos SI e LGPD: Caso o fornecedor não seja aderente aos requisitos apresentados no formulário de avaliação, deve ser realizada uma análise de risco por um comitê diretivo ou de gestão da ARCELORMITTAL GONVARRI para aprovação ou não dos serviços em critério de exceção.

9. Classificação de Fornecedores

Os fornecedores devem ser classificados de acordo com suas necessidades de segurança, como Alta (A), Média (B) e Baixa (C). Esta classificação ajuda a ARCELORMITTAL GONVARRI a alocar recursos adequados e gerenciar riscos.
Alta (A): Fornecedores com acesso a informações altamente sensíveis e sistemas críticos.
Média (B): Fornecedores com acesso a informações importantes, mas não críticas.
Baixa (C): Fornecedores com acesso limitado a informações de baixa sensibilidade.

10. Exemplo de Informações Sensíveis

Propriedade Intelectual: Dados de projetos, inovações e segredos comerciais.
Informações de Clientes: Dados confidenciais relacionados a clientes.
Dados Pessoais: Informações que identifiquem uma pessoa, conforme definido pela LGPD.
Informações Financeiras e Tecnológicas: Detalhes de transações financeiras e configurações de TI.

11. Cumprimento da Política

Esta política assegura que todos os fornecedores da ARCELORMITTAL GONVARRI mantenham altos padrões de segurança da informação, garantindo a proteção dos ativos e a continuidade dos negócios.
O não cumprimento desta política de segurança por parte dos fornecedores pode ser considerado uma infração das suas obrigações e está sujeito a medidas corretivas.

12. Revisão e Atualização

Esta Política será revisada sempre que necessário para refletir mudanças legais ou organizações. Essa atualização será disponibilizada pela ArcelorMittal Gonvarri em:
https://www.portalprivacidade.com.br/arcelormittalgonvarri/fornecedores