Política de Segurança da Informação	PSGSI -001	
	Revisão: 1	Página: 1 de 21

Sumário

1. Objetivo 2
2. Sumário executivo 2
3. Escopo 2
4. Termos e Definições 4
5. Acrônimos 4
6. Regras e Responsabilidades 5
7. Estratégia de gestão de riscos de informação 6
7.1. Avaliação dos Riscos 8
7.2. Propriedades de ativos 9
7.3. Classificação de ativo 9
8. Sistemática de documentação de segurança 9
9. Requisitos de segurança da informação 10
9.1. Organizando a segurança da informação 10
9.2. Gestão de ativos 10
9.2.1. Responsabilidades da área de TI na gestão dos ativos 11
9.3. Segurança de recursos humanos 12
9.4. Segurança Física 12
9.5. Controle de Rede 13
9.5.1 Gestão, comunicação e Operação 13
9.5.2 Datacenter e Backup 14
9.5.3 Controle de acesso 15
9.6. Sistema de informação, aquisição e manutenção 17
9.7. Gestão de incidentes de segurança da informação 17
9.8. Plano de contingência e continuidade de negócios 18
9.9. Conformidade 18
Consequências da Não Conformidade 19
9.10. Violações da Política de Segurança da Informação 19
9.11. Tipos de Violações 19
9.12. Sanções e Penalidades 19
10. Revisão e Melhoria da Política 20
11. Referencias de materiais utilizados 20

© TECNOPLAST Ltda.. Todos os direitos reservados no caso de concessão de patente, modelo, documento ou desenho.
Uma cópia desse documento fora do controle do sistema de gestão de documentos estabelecido, é apenas para o propósito de informação e não é controlado.
A reprodução, distribuição e utilização deste documento, bem como a comunicação de seu conteúdo à terceiros sem autorização são proibidas.

1. Objetivo

2. Sumário executivo

A informação é um ativo da empresa, no contexto de nossa organização, nossos gestores, clientes, concorrentes, fornecedores, governo, mercado financeiro e nossos colaboradores em geral, estão todos tomando decisões de negócios com base nas informações que produzimos, preservamos e publicamos, quer sejamos os proprietários ou responsáveis por sua guarda.

O dia a dia em todas as unidades de negócios da **MUELLER / TECNOPLAST**, está se tornando cada vez mais dependente da tecnologia da informação, para dar-nos suporte às nossas necessidades de informação. A tecnologia não apenas transformou nosso ambiente de negócios, mas também criou novos desafios para o gerenciamento de riscos da informação. Há agora uma aceitação generalizada de que, nesta era da informação, a segurança da informação é imprescindível, vital para o sucesso dos negócios.

A segurança da informação eficaz é essencial para manter a confiança de nossos clientes e parceiros de negócios e para permitir nosso sucesso contínuo em um mundo cada vez mais interconectado e baseado em informações. Também é uma obrigação legal protegermos os dados privados confiados a nós, por nossos parceiros de negócios e colaboradores, garantindo sua integridade, confiabilidade e disponibilidade em tempo hábil.

Por outro lado, as informações privadas e corporativas se tornaram um ativo valioso para nossos concorrentes e alvo de roubo ou furto por meio de programas sofisticados de inteligência. Proteger informações é uma tarefa cada vez mais complexa, desta forma, a **MUELLER / TECNOPLAST** estabelece esta política para a proteção dos ativos de informações apoiada por um programa abrangente de proteção de informações em toda a empresa.

No entanto, todos nós temos a responsabilidade de proteger as informações contra divulgação, alteração ou destruição maliciosa ou acidental, cumprindo o nosso dever:

- Seguirmos os padrões e procedimentos de segurança da informação aplicáveis a nós;
- Mantermos as informações que são confiadas a nós em sigilo;
- Protegermos os dados privados e materiais protegidos por direitos autorais;
- Evitarmos ações e comportamentos que possam colocar em risco nossas redes de dados e nossos ativos de informação;
- Relatarmos qualquer suspeita de abuso ou ameaças potenciais ao nosso pessoal, redes, sistemas ou informações.

Esta Política de Segurança da Informação e seus padrões associados são a base do programa de segurança, para juntos, protegeremos a segurança das informações da **MUELLER / TECNOPLAST**

3. Escopo

Peças Plásticas Injetadas e Montadas para Aplicação em Interiores e Acabamentos Externos, Componentes de Chassis, Motor e Transmissão.

© TECNOPLAST Ltda.. Todos os direitos reservados no caso de concessão de patente, modelo, documento ou desenho.
Uma cópia desse documento fora do controle do sistema de gestão de documentos estabelecido, é apenas para o propósito de informação e não é controlado.
A reprodução, distribuição e utilização deste documento, bem como a comunicação de seu conteúdo à terceiros sem autorização são proibidas.

Esta política e suas normas aplicam-se a todo e qualquer indivíduo com acesso às informações da **MUELLER / TECNOPLAST**, independentemente de seu vínculo com a empresa, como por exemplo: dirigentes, colaboradores efetivos, temporários ou terceirizados, estagiários, clientes, fornecedores. Também se destina a todas as informações criadas, armazenadas, processadas, transmitidas e descartadas ou ativos disponibilizados pela empresa.

As informações existem em muitas formas, pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida fisicamente por correio ou por meios eletrônicos (e-mails, redes sociais, pen drives, etc.), ou exibida em vídeos, fotos ou transmitida verbalmente em conversas formais ou informais. A informação é um ativo que, como outros ativos de negócios importantes, é essencial para o negócio de uma empresa e consequentemente, precisa ser adequadamente protegida e gerida.

As informações, os sistemas de informação e as redes que as processam, enfrentam ameaças à segurança de diversas fontes, incluindo negligência, fraude assistida por computador, vazamento, espionagem, sabotagem, vandalismo, incêndio, inundação, etc. Qualquer que seja a forma da informação, ou meios pelos quais é compartilhada ou armazenada, deve sempre ser protegida de forma adequada. Essa proteção deve ser sempre proporcional ao risco ao qual as informações estão expostas.

A segurança da informação é a proteção da informação contra uma vasta gama de riscos. Inclui os seguintes serviços:

- **Confidencialidade:** serviços que garantem que a informação é observada ou divulgada apenas a quem tem a "necessidade de saber" para cumprir as suas funções ou para cumprir um pedido legal. A confidencialidade garante que a **MUELLER / TECNOPLAST** proteja as informações pessoais e privadas ao limitar estritamente quem as acessa e sobre quais condições e penas;

- **Integridade:** serviços que garantem que as informações sejam protegidas contra modificações não autorizadas (mantendo seu estado original), que as transações comerciais, bem como as trocas de informações dentro da empresa ou com parceiros de negócios, sejam confiáveis como precisas, completas e irrecusáveis (inegociáveis)

- **Disponibilidade:** serviços que garantem que as informações estão disponíveis e utilizáveis quando requisitadas pelas pessoas autorizadas, e os sistemas que fornecem informações são confiáveis e disponíveis quando são necessários, podem resistir a ataques e se recuperar de falhas de forma adequada.

- **Responsabilidade:** serviços que garantem que as ações para acessar, alterar ou excluir informações, ou facilidades de processamento, que podem levar, ou levaram a uma violação de segurança, sejam rastreáveis a uma pessoa física ou jurídica.

A **MUELLER / TECNOPLAST** tem o compromisso de proteger de forma responsável as informações que lhe são confiadas por seus clientes e parceiros de negócios, assim como as geradas por si próprio, equilibrando riscos e custos, com pleno respeito a todas às obrigações legais e à ética empresarial.

A Política de Segurança da Informação cobre todos os ativos de informação da **MUELLER / TECNOPLAST**, sejam em papel ou desmaterializados, onde quer que estejam armazenados ou em trânsito em qualquer tipo de mídia, em todos os sistemas de processamento de informações.

© TECNOPLAST Ltda.. Todos os direitos reservados no caso de concessão de patente, modelo, documento ou desenho.
Uma cópia desse documento fora do controle do sistema de gestão de documentos estabelecido, é apenas para o propósito de informação e não é controlado.
A reprodução, distribuição e utilização deste documento, bem como a comunicação de seu conteúdo à terceiros sem autorização são proibidas.

4. Termos e Definições

Termos	Definições
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.
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.
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.

5. Acrônimos

Termos	Definições
ANPD	Autoridade Nacional de Proteção de Dados é o órgão federal responsável por fiscalizar e aplicar a LGPD, a Lei Geral da Proteção de Dados. Criada em 2018 e sancionada em 2019.
LGPD	Lei Geral de Proteção de Dados.
SDLC	Software Development Life Cycle (SDLC) – Ciclo de Vida de Desenvolvimento de Software.
GCN	Gestão de Continuidade de Negócio é um processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem.
DPI	Direito de Propriedade Intelectual é a área do Direito que, por meio de leis, garante a inventores ou responsáveis por qualquer produção do intelecto, seja nos domínios industrial, científico, literário ou artístico, o direito de obter, por um determinado período de tempo, recompensa pela própria criação.
DPO	Data Protection Officer ou Encarregado de Dados - O encarregado pelo tratamento de dados pessoais possui a função de atuar como canal de comunicação entre instituição, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). IV - Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

© TECNOPLAST Ltda.. Todos os direitos reservados no caso de concessão de patente, modelo, documento ou desenho.
Uma cópia desse documento fora do controle do sistema de gestão de documentos estabelecido, é apenas para o propósito de informação e não é controlado.
A reprodução, distribuição e utilização deste documento, bem como a comunicação de seu conteúdo à terceiros sem autorização são proibidas.

6. Regras e Responsabilidades

A Direção Geral é responsável por:

- Patrocinar, financiar e garantir a aplicabilidade da "Política de Segurança da Informação" pelos funcionários, em cumprimento a todas as leis e obrigações aplicáveis, incluindo a legislação de proteção de dados pessoais, para proteger o negócio, a reputação e interesses legítimos;

- Os gestores deverão manter conduta coerente em relação à segurança da informação, servindo como modelo de conduta para os colaboradores, usuários e prestadores de serviços da **MUELLER / TECNOPLAST**;

- Os gestores deverão disseminar a cultura de cumprimento e respeito a segurança da informação, contribuindo para o entendimento desta política como fundamental para os alicerces da **MUELLER / TECNOPLAST**, preservando o devido acesso, integridade, confidencialidade e disponibilidade;

- Garantir, com o auxílio da área de Recursos Humanos, que nossos colaboradores estejam cientes e orientados sobre a Política de Segurança da Informação, apoiando a aplicação das normas, procedimentos e das boas práticas vigentes para que as cumpram no decorrer de suas atividades, para defender a segurança da informação em conformidade com esta política e agindo prontamente sob quaisquer situações não conformes reais ou potenciais.

O Departamento de TI, sendo o principal setor em relação a Segurança da Informação, é responsável por:

- Implementar esta política e as operações associadas;

- Avaliar a estrutura necessária para o atendimento à Governança de Segurança da Informação, com base em uma metodologia de gerenciamento de risco, para fornecer garantia de que as estratégias de segurança da informação estão alinhadas com os objetivos de negócios, consistentes com as leis aplicáveis e resistentes a ameaças e vulnerabilidades conhecidas;

- Identificar e orçar projetos de aprimoramento de segurança, incluindo ações de preenchimento de lacunas de curto prazo para tratar de questões urgentes de segurança;

- Realizar verificações e testes regulares para obter a garantia de que os direitos de acesso, configurações e parâmetros de segurança de versão estão em conformidade com os requisitos documentados e garantir que a organização tenha a capacidade de responder e se recuperar de eventos de segurança da informação que causem interrupção ou destruição;

- Realizar auditorias regulares com o intuito de avaliar a conformidade com esta política e com os padrões e processos de segurança da informação relacionados;

- Configurar e operar as tecnologias de segurança da informação adequadas;

- Garantir que os Planos de Recuperação de Desastres de TI (Plano de Contingência) sejam adequados à finalidade na estrutura geral do Gerenciamento de Continuidade de Negócios Corporativos.

O Departamento de SGI é responsável por:

- Garantir que todos os procedimentos operacionais sejam documentados e executados de acordo com a orientação de implementação do padrão de segurança de informações;

© TECNOPLAST Ltda.. Todos os direitos reservados no caso de concessão de patente, modelo, documento ou desenho.
Uma cópia desse documento fora do controle do sistema de gestão de documentos estabelecido, é apenas para o propósito de informação e não é controlado.
A reprodução, distribuição e utilização deste documento, bem como a comunicação de seu conteúdo à terceiros sem autorização são proibidas.

O departamento de Recursos Humanos é responsável por:

- Definir e comunicar esta política dentro da organização, bem como o monitoramento e comunicação às partes interessadas sobre a conformidade da empresa;
- Implementar uma forma de contratação de novos colaboradores por meio de entrevistas, testes e, posteriormente, treinamentos com relação a Segurança da Informação, validando a competência singular.
- Apoiar e disseminar a cultura de segurança adequada na organização, conduzindo um programa de treinamento e conscientização da Segurança da Informação;
- Implementar os controles físicos e os requisitos de segurança para a adequada gestão de acessos prediais.
- **Todos os colaboradores, usuários, prestadores de serviços, fornecedores, são responsáveis por:**

Entende-se por colaboradores, usuários, prestadores de serviços, fornecedores, toda e qualquer pessoa física ou jurídica, que exerça alguma atividade interna ou externa para **MUELLER / TECNOPLAST**

- Seguir e cumprir esta Política de Segurança da Informação e suas definições;
- Reportar, sem exceção, quaisquer violações ou suspeita de violação e incidentes que possam infringir a Política de Segurança da Informação ou de seus padrões e práticas e procedimentos de apoio ao seu gestor ou ao responsável por segurança da informação da **MUELLER / TECNOPLAST**;
- Usar as informações, redes, aplicativos, sistemas da **MUELLER / TECNOPLAST**, bem como por todas as comunicações que criem ou enviem, seja qual for o seu status de funcionário;
- Não realizar acessos indevidos e não compartilhar informações confidenciais da empresa, pois estão sujeitos às **penalidades legais cabíveis**, de acordo com o **Código de Ética e Conduta**, quer seja específico ou integrado aos demais contratos assinados no momento da contratação.

7. Estratégia de gestão de riscos de informação

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

© TECNOPLAST Ltda.. Todos os direitos reservados no caso de concessão de patente, modelo, documento ou desenho.
Uma cópia desse documento fora do controle do sistema de gestão de documentos estabelecido, é apenas para o propósito de informação e não é controlado.
A reprodução, distribuição e utilização deste documento, bem como a comunicação de seu conteúdo à terceiros sem autorização são proibidas.

SGSI

© TECNOPLAST Ltda.. Todos os direitos reservados no caso de concessão de patente, modelo, documento ou desenho.
Uma cópia desse documento fora do controle do sistema de gestão de documentos estabelecido, é apenas para o propósito de informação e não é controlado.
A reprodução, distribuição e utilização deste documento, bem como a comunicação de seu conteúdo à terceiros sem autorização são proibidas.

7.1. Avaliação dos Riscos

A avaliação de risco é o processo para compreender e quantificar o impacto comercial de uma violação de segurança, criada por uma ameaça que explora vulnerabilidades.

Risco = Ameaças x Vulnerabilidades x **Impactos**

Ameaças: aquelas que enfrentamos se enquadram em três grandes categorias:

- **Ameaças acidentais:** erros humanos, negligência, falhas de processo ou sistema, desastres físicos (incêndios, inundações, queda de aeronaves, colisão de veículos), desastres naturais (tempestades, terremotos, descargas elétricas), etc.;
- **Ameaças malévolas internas:** funcionários descontentes, vingança, suborno, corrupção, etc.;
- **Ameaças malévolas externas:** vandalismo, desfiguração de sites ou sistemas, sabotagens, invasões de hackers, guerras, extorsões cibernéticas (ramsonwares), phishing, etc.

A análise de ameaças deve considerar a motivação, capacidade e acessibilidade das fontes potenciais de ameaça e o catalisador potencial para determinar a probabilidade de uma ameaça específica.

Vulnerabilidades: existem onde há alguns pontos fracos em um ser humano, processo ou sistema que podem ser explorados por uma ameaça.

Impactos: é o efeito geral que uma ameaça teria sobre nossos ativos e negócios ao explorar vulnerabilidades. Isso pode resultar em:

- Danos de ordem pessoal;
- Perdas financeiras;
- Ações de ordem legal;
- Continuidade dos negócios abalada;
- Redução da confiança do cliente;
- Posição competitiva reduzida;
- Reputação comprometida.

O objetivo do gerenciamento de risco é fornecer a garantia de que o risco aos ativos e recursos de informação está sendo gerenciado de forma adequada da maneira mais econômica. As opções possíveis para gerenciamento de risco são:

- Aceitar os riscos de forma consciente e objetiva (desde que satisfaçam claramente todas as obrigações legais);
- Evitar os riscos, não permitindo ações que fariam com que os riscos ocorressem;
- Transferir os riscos para outras partes, por ex. seguradoras ou fornecedores;
- Implementar controles apropriados para reduzir os riscos a um nível aceitável.

© TECNOPLAST Ltda.. Todos os direitos reservados no caso de concessão de patente, modelo, documento ou desenho.
Uma cópia desse documento fora do controle do sistema de gestão de documentos estabelecido, é apenas para o propósito de informação e não é controlado.
A reprodução, distribuição e utilização deste documento, bem como a comunicação de seu conteúdo à terceiros sem autorização são proibidas.

7.2. Propriedades de ativos

A Tecnologia da Informação (TI) evoluiu de uma função crítica de retaguarda para um facilitador de negócios na linha de frente mais visível. Os serviços baseados na Web e a desmaterialização das informações nos levam a confiar cada vez mais as funções críticas de negócios à TI.

No entanto, as informações permanecem propriedade da empresa ou de seus parceiros de negócios. A prestação de contas e a responsabilidade estão ligadas à propriedade, assim como a autoridade. É responsabilidade do proprietário e depositário da informação avaliar adequadamente a exposição ao risco de suas informações, decidir e implementar a estratégia de gerenciamento de risco apropriada para lidar com esses riscos.

Consequentemente, todos os ativos e recursos de informação devem ter um proprietário nomeado, conforme definido na planilha de análise de riscos de segurança da informação:

- Responsável pela segurança lógica e física dos ativos / recursos de informação;
- Responsável se a segurança do ativo / recurso de informações for comprometida.

7.3. Classificação de ativo

O proprietário deve garantir que todos os ativos e recursos de informação sejam classificados em termos de confidencialidade, integridade, disponibilidade e responsabilidade. O esquema de classificação é projetado com base no impacto de uma violação do serviço de segurança relacionado.

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

8. Sistemática de documentação de segurança

Esta Política de Segurança da Informação define **PORQUE** a segurança é importante e qual deve ser o nível geral esperado de segurança da informação. Ela especifica o lema da gestão executiva e fornece declarações de política da alta direção. Ela representa a declaração de compromisso da empresa em relação à segurança da informação.

Os Padrões de Segurança da Informação definem **QUAIS** tipos de controles de segurança da informação devem ser implementados, orientam a implementação dos controles de segurança da informação e fornecem o endosso gerencial da

© TECNOPLAST Ltda.. Todos os direitos reservados no caso de concessão de patente, modelo, documento ou desenho.
Uma cópia desse documento fora do controle do sistema de gestão de documentos estabelecido, é apenas para o propósito de informação e não é controlado.
A reprodução, distribuição e utilização deste documento, bem como a comunicação de seu conteúdo à terceiros sem autorização são proibidas.

política de segurança da informação de alto nível. Os documentos de segurança detalhados subsequentes especificam **COMO** os controles de segurança são implementados. Eles são agrupados em três categorias:

- Práticas de segurança humana;
- Procedimentos de segurança operacional;
- Padrões técnicos de segurança.

A **MUELLER / TECNOPLAST** adotou os padrões da norma **do TISAX VDA 5.1** como o principal padrão de referência para desenvolver o seu Sistema de Gestão de Segurança da Informação.

9. Requisitos de segurança da informação

9.1. Organizando a segurança da informação

Um plano estratégico de segurança da informação corporativa deve ser definido, obter suporte executivo e implementado. Recursos e orçamento adequados devem ser alocados. Um comitê de coordenação deve ser estabelecido para facilitar sua implementação, e coordenado sob a responsabilidade dos gerentes departamentais.

9.2. Gestão de ativos

Todos os ativos de informação e tecnologia da informação da **MUELLER / TECNOPLAST** devem ser claramente identificados, inventariados e ter um proprietário identificado que é responsável por sua proteção.

Embora as responsabilidades do proprietário do ativo possam ser delegadas à pessoa mais adequada na organização, a responsabilidade final pelas ações tomadas, decisões tomadas e conformidade permanece com o proprietário do ativo;

- Um sistema de classificação de segurança deve ser implementado e usado para definir um conjunto apropriado de níveis de proteção de segurança e para comunicar aos usuários a necessidade de medidas especiais de tratamento (conforme item 7.3);

- As informações confidenciais só devem ser divulgadas para funcionários autorizados ou terceiros com base na 'necessidade de saber' e após a assinatura de um Acordo de Não Divulgação;

- Os equipamentos disponibilizados aos colaboradores, usuários e prestadores de serviços, são de propriedade da **MUELLER / TECNOPLAST** cabendo a cada um utilizá-los e manuseá-los corretamente para

© TECNOPLAST Ltda.. Todos os direitos reservados no caso de concessão de patente, modelo, documento ou desenho.
Uma cópia desse documento fora do controle do sistema de gestão de documentos estabelecido, é apenas para o propósito de informação e não é controlado.
A reprodução, distribuição e utilização deste documento, bem como a comunicação de seu conteúdo à terceiros sem autorização são proibidas.

as atividades de desenvolvimento de seu trabalho, bem como cumprir as recomendações constantes nos procedimentos operacionais;

- É proibido qualquer procedimento de manutenção física ou lógica, instalação, remoção, configuração ou modificação, sem o conhecimento prévio e o acompanhamento da área de TI, ou de quem este determinar;

- Todas as atualizações e correções de segurança do sistema operacional ou aplicativos críticos conforme lista definida, somente poderão ser realizadas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor;

- Os sistemas e computadores devem ter versões do software antivírus instaladas, ativas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a área de TI;

- Os ativos da **MUELLER / TECNOPLAST** deverão ser inventariados no mínimo a cada 12 meses;

- O acesso e uso dos ativos (computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física), será através de conta individual sob controle da Área de TI, cujo acesso, a este responsável, somente poderá ser liberado mediante assinatura (física ou eletrônica) de um Termo de Responsabilidade em consonância com esta Política de Segurança de Informação, com as seguintes observâncias:

    - Os códigos de usuários (ID Logins) individuais atribuídos aos nossos colaboradores são de responsabilidade dos próprios colaboradores;

    - Os códigos de usuários (ID Logins) atribuídos a terceiros são de responsabilidade do próprio terceiro, solidariamente com o gestor da área contratante;

    - O acesso aos ambientes administrativos (escritórios) é bloqueado para qualquer colaborador, usuário e prestador de serviço que não faça parte do grupo de colaboradores com funções administrativas.

9.2.1. Responsabilidades da área de TI na gestão dos ativos

- Garantir que em caso de ausência de atividade nos computadores da **MUELLER / TECNOPLAST**, a proteção de tela seja ativada com senha;

- Garantir o bloqueio de adição de componentes ao Sistema Operacional (SO), como ferramentas de edição do Registros do SO, alteração do nome da máquina e compartilhamento de arquivos ou pastas das máquinas para usuários comuns;

- Definir as regras formais para instalação de software e hardware em ambiente de produção;

- Garantir a disponibilização em ambiente seguro do uso, manuseio, guarda de assinatura e certificados digitais;

- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências;

© TECNOPLAST Ltda.. Todos os direitos reservados no caso de concessão de patente, modelo, documento ou desenho.
Uma cópia desse documento fora do controle do sistema de gestão de documentos estabelecido, é apenas para o propósito de informação e não é controlado.
A reprodução, distribuição e utilização deste documento, bem como a comunicação de seu conteúdo à terceiros sem autorização são proibidas.

- Garantir, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa, bem como processo de exclusão de dados ou mídias das máquinas quando de utilização por um novo usuário**;**

- Bloquear acessos de dispositivos a rede local, tais como celulares, notebooks, pen drives, discos removíveis e instalação de impressoras externas;

- Manter todos os softwares de proteção contra ameaças em geral, atualizados conforme as recomendações e exigências dos fabricantes em todos computadores, notebooks, celulares e demais equipamentos de gerenciamento de rede (firewalls, roteadores, etc.);

- Monitorar o ambiente de TI, gerando históricos de evidências e controles, planejando e executando ações preventivas e corretivas.

9.3. Segurança de recursos humanos

A **MUELLER / TECNOPLAST** colocará em prática controles e medidas adequadas para garantir que apenas contrate e disponha de pessoas cuja atitudes e perfis sejam compatíveis com a importância que atribui à segurança da informação.

A **MUELLER / TECNOPLAST** conduzirá um programa de conscientização de segurança para garantir que todos os funcionários estejam cientes dos riscos, políticas, práticas e contramedidas de segurança da informação;

- Todos os funcionários devem usar os sistemas de processamento de informações **MUELLER / TECNOPLAST** para fins comerciais de forma consistente com o "Código de Etica + Contrato de trabalho da **MUELLER / TECNOPLAST**";

- A empresa deve finalmente garantir que, ao rescindir o contrato ou acordo de trabalho, ou alterar responsabilidades ou funções, funcionários e terceiros usuários, devolvam todos os ativos e equipamentos da **MUELLER / TECNOPLAST** confiados a eles de forma controlada. E tenham todos os direitos de acesso atuais às informações e recursos de processamento de informações removidos.

9.4. Segurança Física

A **MUELLER / TECNOPLAST** irá definir, implementar e gerenciar as medidas de segurança física adequadas para proteger seus funcionários e ativos físicos.

- Edifícios que abrigam sistemas de informação devem ser adequadamente protegidos com perímetros de segurança para prevenir qualquer acesso não autorizado;

- Os controles de entrada devem garantir que apenas pessoas autorizadas tenham acesso permitido;

- Instalações de apoio de áreas seguras e salas de informática, incluindo fornecimento de eletricidade, geradores, nobreaks, aquecimento e ar-condicionado, abastecimento de água e fornecimento de telecomunicações, devem ser controlados e devem ser redundantes para evitar o risco de interrupção e consequências em equipamentos de alta disponibilidade;

- Para os equipamentos considerados como críticos devem ser mantidos adequadamente com suporte adequado, de acordo com as recomendações do fornecedor;

© TECNOPLAST Ltda.. Todos os direitos reservados no caso de concessão de patente, modelo, documento ou desenho.
Uma cópia desse documento fora do controle do sistema de gestão de documentos estabelecido, é apenas para o propósito de informação e não é controlado.
A reprodução, distribuição e utilização deste documento, bem como a comunicação de seu conteúdo à terceiros sem autorização são proibidas.

- A eliminação ou reutilização de sistemas de processamento de informações deve seguir um controle restrito para impedir o acesso de informações confidenciais por uma pessoa não autorizada

- Uma política de mesa limpa e uma política de tela limpa "Código de Prática para o uso aceitável dos Sistemas de Processamento de Informação" deve ser promovida para evitar roubo oportunista ou divulgação de informações confidenciais;

- O equipamento fora de uso deve ser desconectado e o tempo limite da sessão implementado;

- As impressoras e fotocopiadoras usados para informações confidenciais não devem imprimir diretamente sem a proteção de usuário e senha a serem identificados de maneira presencial, durante a impressão;

- Garantir o registro de novos colaboradores, usuários e prestadores de serviços junto às Portarias de Acesso;

- Prover acesso deles às Portarias de Acesso através de crachá;

- Dar ciência aos colaboradores que todo e qualquer dispositivo de identificação pessoal não poderá ser compartilhado com outras pessoas em hipótese alguma;

- Em caso de rescisão contratual, perda ou roubo do crachá de acesso físico, cancelar o acesso o mais breve possível e formalizar junto ao departamento de recursos humanos. Para o caso de acesso via digital, bloquear à identificação;

- Terceiros contratados deverão ser cadastrados nas ferramentas de segurança física do mesmo modo que colaboradores, usuários e prestadores de serviços;

- Garantir a gestão do contrato de monitoramento interno e perímetros da empresa, através de câmeras de segurança dispostas nas áreas determinadas no mapeamento de riscos de segurança, possibilitando a recuperação de imagens em caso de sinistro ou incidentes, no período mínimo de 10 dias de retenção;

- Gerir os serviços de manutenção e testes periódicos de Nobreaks e Geradores (quando aplicável). Para o caso de testes documentar devidamente para eventuais auditorias;

- Gerir o contrato de links de comunicações, garantindo redundância entre site e provedores diferentes.

9.5. Controle de Rede

9.5.1 Gestão, comunicação e Operação

As instalações de comunicações e operações serão gerenciadas de acordo com as melhores práticas de mercado. A documentação formal da infraestrutura de TI e os procedimentos de suporte são componentes cruciais para garantir operações e comunicações perenes e seguras.

- Os procedimentos e responsabilidades operacionais devem ser documentados formalmente. Esses procedimentos devem ser classificados de acordo com o esquema de classificação, gerenciados de acordo e sujeitos ao processo de controle de mudanças;

- As instalações de desenvolvimento e teste devem ser separadas dos sistemas de produção, para reduzir o risco de instabilidade operacional ou modificações não autorizadas;

Uma cópia desse documento fora do controle do sistema de gestão de documentos estabelecido, é apenas para o propósito de informação e não é controlado.
A reprodução, distribuição e utilização deste documento, bem como a comunicação de seu conteúdo à terceiros sem autorização são proibidas.

- Os utilitários do sistema devem ser removidos por padrão de todos os sistemas de produção;

- Relacionamentos com fornecedores terceirizados contratados para fornecer serviços de TI devem ser formalmente documentados e gerenciados. Indicadores Chave de Desempenho (KPI) e Acordos de Nível de Serviço (SLA) devem ser definidos e monitorados. Devem ocorrer reuniões regulares de gerenciamento para revisar o desempenho do terceiro em relação aos SLA's e concordar com as ações corretivas/preventivas exigidas;

- Critérios de aceitação para novos sistemas de informação, atualizações e novas versões devem ser estabelecidos. Testes adequados dos sistemas devem realizados antes da instalação em produção;

- Todos os sistemas, servidores (quando aplicável) e estações de trabalho devem estar equipados com sistemas antivírus, verificando todos os arquivos inseridos no sistema por qualquer meio (mídia removível, rede, e-mail ...). Deve haver um processo para atualizar automaticamente o arquivo de definição de vírus de acordo com a recomendação do fornecedor. O procedimento deve estar disponível para usuários remotos e em viagem. Todas as mídias removíveis devem ser verificadas em busca de vírus quando reconectadas aos sistemas de informação;

- Deve-se fazer backup das informações para garantir a disponibilidade das informações e dos sistemas de suporte. A mídia de backup deve ser protegida de acordo com os padrões de classificação de informações. A mídia de backup deve ser testada regularmente de acordo com as recomendações do fabricante. O procedimento de restauração deve ser formalmente documentado e testado. A mídia de backup deve ser e armazenada em edificações fisicamente separadas e distantes dos Datacenters que concentram os bancos de dados e servidores de arquivos de todos os processos críticos da **MUELLER / TECNOPLAST**;

- Todo o tráfego da Internet deve ser filtrado pelos firewalls configurados nas redes **MUELLER / TECNOPLAST** e os modens e outros meios de acesso à Internet fora dos controles de firewall, ou qualquer rede IP externa, são proibidos. Varreduras periódicas devem ser realizadas para detectar tais conexões IP. Roteadores não registrados e não autorizados devem ser removidos imediatamente;

- Todas as informações publicadas nos sites da **MUELLER / TECNOPLAST** estão sujeitas à aprovação formal da Diretoria e apenas implementado pelo DPO (Data Protection Officer). Os dados do cliente coletados no site, ou por qualquer outro meio, devem estar sujeitos aos controles apropriados, de acordo com a Lei Geral de Proteção de Dados (LGPD), conforme exigido pela ANPD.

9.5.2 Datacenter e Backup

As instalações de comunicações e operações serão gerenciadas de acordo com as melhores práticas, sendo responsabilidade do TI garantir que as seguintes regras se apliquem, no que diz respeito ao controle do Datacenter, sendo:

- O acesso ao Datacenter fica restrito aos colaboradores, usuários e prestadores de serviços designados e habilitados por biometria com lista de controle de liberação;

- Todo acesso ao Datacenter deverá ser registrado por nome, data e hora;

- Qualquer terceiro ou prestador de serviço somente poderá acessar o datacenter em situações imprescindíveis e acompanhado por um dos colaboradores designados para administrar os processos de segurança da informação, mantendo o histórico de acessos do terceiro à área;

© TECNOPLAST Ltda.. Todos os direitos reservados no caso de concessão de patente, modelo, documento ou desenho.
Uma cópia desse documento fora do controle do sistema de gestão de documentos estabelecido, é apenas para o propósito de informação e não é controlado.
A reprodução, distribuição e utilização deste documento, bem como a comunicação de seu conteúdo à terceiros sem autorização são proibidas.

- O Datacenter deverá ser mantido limpo e organizado, não sendo permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável;

- A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com o preenchimento da solicitação de liberação pelo colaborador, usuário ou prestador de serviços solicitante mediante a autorização formal desse instrumento pelo responsável do datacenter e um membro da diretoria seguindo o procedimento da controladoria de gestão de ativos.

- No caso de desligamento de colaboradores, usuários ou prestadores de serviços que possuam acesso ao Datacenter, deverá ser providenciada de imediato a sua exclusão do sistema de autenticação vigente e da lista de colaboradores autorizados.

É responsabilidade do TI garantir que as seguintes regras se apliquem no que diz respeito à geração de Backup dos dados da rede interna, sendo:

- Os backups devem ser automáticos e executados preferencialmente fora do horário comercial, nas chamadas "janelas de backup" – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática, salvo os backup's de banco de dados que serão realizados de hora em hora;

- Os backups ficam armazenados em nuvem e garantidos por contrato com fornecedor representativo no mercado, seguindo boas práticas de gestão de serviços e segurança da informação.

- O tempo de retenção dos backups deverá ser definido conforme o resultado da análise de riscos realizada, liderada pelo TI com os diversos departamentos da empresa, a fim de avaliar e atender as exigências legais, específicas de nossos clientes e partes interessadas.

9.5.3 Controle de acesso

A política de controle de acesso da **MUELLER / TECNOPLAST**, que especifica os procedimentos de identificação, registro, autenticação e autorização do usuário é aplicável a todas as informações, sistemas de processamento de informações, redes e acessos.

Todo colaborador, usuário e prestador de serviços terá acesso a login e senha individual, com alteração periódica e monitorado através de processos da área de TI. É de responsabilidade de cada colaborador a proteção e não compartilhamento de sua senha individual, ficando sujeito as penalidades administrativas e legais pelo uso indevido, de acordo com Código de conduta e contrato de trabalho assinado pelo mesmo.

Para tanto é diretriz da política de segurança da informação os seguintes pontos:

- Uma convenção de nomenclatura de usuário padrão;

- Um procedimento de registro e cancelamento de registro do usuário, incluindo atividades de manutenção para manter os direitos e privilégios de acesso durante o ciclo de vida da conta;

- Um procedimento de autorização formal para aprovar os direitos de acesso do usuário;

- Um procedimento de autenticação;

© TECNOPLAST Ltda.. Todos os direitos reservados no caso de concessão de patente, modelo, documento ou desenho.
Uma cópia desse documento fora do controle do sistema de gestão de documentos estabelecido, é apenas para o propósito de informação e não é controlado.
A reprodução, distribuição e utilização deste documento, bem como a comunicação de seu conteúdo à terceiros sem autorização são proibidas.

- Os usuários são responsáveis pelo gerenciamento seguro de suas senhas. A senha é o bem mais valioso de cada usuário de TI da **MUELLER / TECNOPLAST** Ninguém está autorizado a pedir a alguém que revele sua senha e ninguém precisa solicitá-la. Qualquer tentativa de descobrir uma senha ou qualquer divulgação de uma senha será considerada uma violação de segurança e gerenciada de acordo;

- O acesso de fornecedores e técnicos de manutenção às portas de diagnóstico e configuração remotas do sistema deve estar sujeito à política de controle de acesso da empresa. Esses controles devem ser especificados no contrato de manutenção.

- O uso do correio eletrônico é para fins corporativos e relacionados às atividades do colaborador, usuário e prestador de serviços vinculados a **MUELLER / TECNOPLAST**;

- Mensagens enviadas via correio eletrônico são criptografadas de acordo com a política do mensageiro de emails vigentes.

- Todas as mensagens transmitidas através do e-mail da **MUELLER / TECNOPLAST** possuem backup e podem ser recuperadas, com observância de prazo contratado, possibilitando o resgate do histórico total;

- Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da **MUELLER / TECNOPLAST**, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação;

- Os colaboradores, usuários e prestadores de serviços não estão autorizados a falar em nome da **MUELLER / TECNOPLAST** para quaisquer meios de comunicação (imprensa, TV, rádio, etc.) sem a devida e expressa autorização da diretoria e /ou presidência, não poderão também manifestar-se, seja por e-mail, entrevista on-line, podcast, redes sociais, seja por documento físico, entre outros;

- Os colaboradores, usuários e prestadores de serviços não estão autorizados a copiar, captar, imprimir ou enviar imagens das telas para terceiros, devendo atender os regulamentos internos de uso de imagens, à Lei de Direitos Autorais, e à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais;

- Os colaboradores, usuários e prestadores de serviços não estão autorizados a copiar, captar, imprimir ou enviar para terceiros, sem autorização expressa da Diretoria, qualquer tipo de documento, relatório, ou mesmo aqueles considerados “rascunhos”, para devendo atender os regulamentos internos de uso de imagens, à Lei de Direitos Autorais, e à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais:

- É proibida a divulgação ou o compartilhamento de informações da **MUELLER / TECNOPLAST** em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet;

- Os colaboradores, usuários e prestadores de serviços, com acesso à internet, não estão autorizados a fazer o download (baixa de arquivos) de qualquer natureza. Eventual necessidade do usuário, para o desenvolvimento de suas atividades, deverá ser submetida a liberação pela Área de TI;

- O download e a utilização de programas de entretenimento e jogos são terminantemente proibidos;

Como regra geral, é terminantemente proibido e não será tolerado, qualquer armazenamento, distribuição, edição, impressão ou gravação, por qualquer recurso, de materiais de cunho sexual, pedofilia, racismo e/ou homofóbico,

© TECNOPLAST Ltda.. Todos os direitos reservados no caso de concessão de patente, modelo, documento ou desenho.
Uma cópia desse documento fora do controle do sistema de gestão de documentos estabelecido, é apenas para o propósito de informação e não é controlado.
A reprodução, distribuição e utilização deste documento, bem como a comunicação de seu conteúdo à terceiros sem autorização são proibidas.

perseguição religiosa ou política, bem como degradantes em geral e/ou que de alguma forma firam as normas do Código de Ética e Conduta da **MUELLER / TECNOPLAST**

Maiores informações também consultar "Código de Etica "Aceitável dos Sistemas de Processamento de Informação" e "Política de Gerenciamento de Senha".

9.6. Sistema de informação, aquisição e manutenção

A metodologia de aquisição de sistemas de informação deve incluir um processo formal para identificar, documentar e implementar os controles de segurança necessários. Esses controles devem ser proporcionais aos riscos identificados resultantes do processo de gestão de riscos e do esquema de classificação de ativos;

- O processamento do aplicativo deve incluir controles para garantir o processamento correto das informações, desde validação de dados de entrada, proteção de integridade de código, integridade de mensagens e verificação de saída. Esses controles devem estar alinhados com a classificação do sistema;

- As alterações no nível do sistema operacional devem ser validadas em relação aos aplicativos para garantir que não haja conflito ou instabilidade induzida;

- Um processo formal deve ser definido e responsabilidades atribuídas para monitorar vulnerabilidades, técnicas, ciclo de lançamento do fornecedor e patches / hot fixes de segurança. O processo deve identificar os critérios para instalação de correções e atualizações, levando em consideração o melhor equilíbrio entre a eficiência operacional e a mitigação de riscos de segurança;

- Os sistemas operacionais e pacotes padrão devem ser reforçados e os serviços não utilizados eliminados. O valor padrão de todos os parâmetros de segurança deve ser revisado e especificado de acordo com a classificação do sistema.

9.7. Gestão de incidentes de segurança da informação

Processos e instalações devem ser implementados para detectar desvios, agregar e correlacionar eventos anormais e fornecer relatório gerencial. Todas as falhas, detectadas por um sistema ou relatadas por um usuário, devem ser registradas e investigadas. Os registros de auditoria devem ser protegidos para, eventualmente, serem usados como evidência em caso de investigações forenses.

Todos os funcionários e usuários terceirizados devem relatar todos os incidentes e fragilidades de segurança da informação detectados ou suspeitos ao seu gestor imediato ou ao responsável de TI;

- Deve haver um procedimento para classificar os incidentes relatados de acordo com seu impacto nos negócios para determinar a urgência de uma ação e atribuir as habilidades certas para conduzir uma investigação. O procedimento deve respeitar a regulamentação aplicável à proteção de dados privados;

- O procedimento de tratamento do incidente deve ser documentado e deve incluir, dependendo da classificação do incidente, etapas para classificação do incidente, contenção do impacto, erradicação da causa raiz, recuperação de informações e análise pós finalizado;

- Se o incidente for suspeito de ser criminoso e exigir ações legais, possivelmente para um tribunal de justiça, as evidências do incidente devem ser protegidas.

© TECNOPLAST Ltda.. Todos os direitos reservados no caso de concessão de patente, modelo, documento ou desenho.
Uma cópia desse documento fora do controle do sistema de gestão de documentos estabelecido, é apenas para o propósito de informação e não é controlado.
A reprodução, distribuição e utilização deste documento, bem como a comunicação de seu conteúdo à terceiros sem autorização são proibidas.

9.8. Plano de contingência e continuidade de negócios

A Gestão de Continuidade de Negócio (GCN) permite que a empresa continue os processos de negócios essenciais em um nível aceitável, apesar de uma interrupção da função de negócios. O GCN deve garantir que todos os processos de negócios críticos, incluindo suas infraestruturas e sistemas de TI de suporte, informações, equipe, parceiros, área de trabalho, sejam identificados, inventariados e possam retomar as atividades em caso de desastre, em um tempo pré-definido e acordado por meio de alternativas possíveis em procedimentos de trabalho.

O GCN deve garantir que um nível aceitável de qualidade e segurança continue a ser garantido durante a operação em condições de desastre. Deve incluir um cenário de "retorno ao normal" e deve ser validado para fornecer garantia de gerenciamento de sua resiliência.

A **MUELLER / TECNOPLAST** deve manter um Plano de Contingência vigente, documentado, divulgado e revisado anualmente. O Plano de Contingência tem como objetivo garantir a continuidade dos serviços prestados em caso de impossibilidade de acesso dos colaboradores, usuários e prestadores de serviços ao espaço físico de trabalho.

O Plano de contingência e continuidade de negócios deve cobrir os pontos abaixo:

- **Contingências de infraestruturas físicas:** assim compreendidas as situações de catástrofes naturais ou não, tais como inundações, incêndios, desabamentos e etc. que impeçam o acesso e/ou utilização das instalações da **MUELLER / TECNOPLAST**, como também danos físicos relevantes a instalações e/ou equipamentos, intencionais ou não e ainda falhas no fornecimento de energia elétrica;

- **Contingências de infraestruturas tecnológicas:** compreendidas as situações de inacessibilidade, falha ou perda de quaisquer recursos de TI, tais como hardware, software, telecom, rede e segurança.

O Plano de contingência deve estabelecer os procedimentos a serem adotados pela **MUELLER / TECNOPLAST** e seus colaboradores, usuários e prestadores de serviços em caso de eventos relacionados a impossibilidade de acesso físico ou tecnológico, seja por eventos de greve, pandemia, bloqueios de acesso ao prédio ou problemas na infraestrutura ou ainda por desastres de força maior.

9.9. Conformidade

É política da **MUELLER / TECNOPLAST**, cumprir todos os requisitos legislativos, estatutários e contratuais pertinentes aos requisitos de informação e sistemas de informação.

- A **MUELLER / TECNOPLAST** implementa a proteção de dados privados e privacidade conforme especificado pela Lei Geral Proteção de Dados (LGPD);

- A **MUELLER / TECNOPLAST** respeita os direitos de propriedade intelectual (DPI) de outras organizações e usa apenas cópias e licenças legais de software;

- Os registros da **MUELLER / TECNOPLAST** devem ser protegidos contra perda, destruição e falsificação. Eles devem ser classificados e identificados por um período de retenção do arquivo por tipo de registro.

© TECNOPLAST Ltda.. Todos os direitos reservados no caso de concessão de patente, modelo, documento ou desenho.
Uma cópia desse documento fora do controle do sistema de gestão de documentos estabelecido, é apenas para o propósito de informação e não é controlado.
A reprodução, distribuição e utilização deste documento, bem como a comunicação de seu conteúdo à terceiros sem autorização são proibidas.

Consequências da Não Conformidade

9.10. Violações da Política de Segurança da Informação

A **MUELLER / TECNOPLAST** está comprometida em manter a segurança de suas informações confidenciais e recursos de tecnologia da informação. Qualquer violação da Política de Segurança da Informação será tratada com a devida seriedade.

9.11. Tipos de Violações

As violações da Política de Segurança da Informação podem incluir, mas não se limitam a:

a) Acesso não autorizado a sistemas, redes ou informações confidenciais.

b) Divulgação não autorizada de informações confidenciais.

c) Uso indevido de recursos de TI da empresa.

d) Falha em relatar incidentes de segurança da informação.

e) Qualquer ação que coloque em risco a integridade, confidencialidade ou disponibilidade das informações.

9.12. Sanções e Penalidades

As violações da Política de Segurança da Informação estarão sujeitas a sanções e penalidades, dependendo da gravidade da violação e das circunstâncias envolvidas. As sanções e penalidades podem incluir, mas não estão limitadas a:

a) **Aviso formal:** Para violações menores ou não intencionais, a primeira ação pode ser um aviso formal.

b) **Treinamento obrigatório:** Para violações leves, os funcionários podem ser obrigados a passar por treinamento adicional em segurança da informação.

c) **Suspensão de acesso:** Em casos de violações graves, o acesso a sistemas, redes ou informações confidenciais pode ser temporariamente suspenso.

d) **Demissão:** Violações graves ou repetidas podem resultar na demissão do funcionário.

e) **Ações legais:** Quando necessário, a empresa pode tomar medidas legais contra o indivíduo responsável.

f) **Responsabilidade civil e criminal:** Ações legais civis ou criminais podem ser buscadas, dependendo das circunstâncias da violação.

g) **Multas e penalidades financeiras:** Em conformidade com regulamentações de privacidade e segurança de dados, a organização pode ser obrigada a pagar multas substanciais se ocorrer uma violação de dados devido à negligência.

A decisão sobre a sanção ou penalidade a ser aplicada será tomada pelo **Comitê da Segurança de Informação e Privacidade** estabelecido, juntamente com a **Direção e Gestão**, levando em consideração a gravidade da violação e as circunstâncias específicas.

© TECNOPLAST Ltda.. Todos os direitos reservados no caso de concessão de patente, modelo, documento ou desenho.
Uma cópia desse documento fora do controle do sistema de gestão de documentos estabelecido, é apenas para o propósito de informação e não é controlado.
A reprodução, distribuição e utilização deste documento, bem como a comunicação de seu conteúdo à terceiros sem autorização são proibidas.

10. Revisão e Melhoria da Política

A **MUELLER / TECNOPLAST** se reserva o direito de revisar e melhorar esta Política de Segurança da Informação a cada um ano. A eficácia do sistema de gestão de segurança da informação será revisada como parte desse processo.

11. Referencias de materiais utilizados

- ABNT NBR ISO/IEC 27001:2013/2022
- ABNT NBR ISO/IEC 27002:2013/2022
- LGPD Lei nº 13.709, de 14 de agosto de 2018
- VDA ISA 6.0.3

© TECNOPLAST Ltda.. Todos os direitos reservados no caso de concessão de patente, modelo, documento ou desenho.
Uma cópia desse documento fora do controle do sistema de gestão de documentos estabelecido, é apenas para o propósito de informação e não é controlado.
A reprodução, distribuição e utilização deste documento, bem como a comunicação de seu conteúdo à terceiros sem autorização são proibidas.

ELABORAÇÃO / APROVACÃO

Elaborado:	Aprovado:	Data:
Fabyo Guimarães	Pablo Rabachini	22/05/2024
Elaborado:	**Aprovado:**	**Data:**
Fabyo Guimarães	Pablo Rabachini	21/04/2025

CONTROLE DE REVISÕES

Nº. da Revisão	Data	Descrição da Alteração
0	22/05/2024	Emissão inicial
1	21/04/2025	Revisão para adequação de termos e alinhamento com a nova versão do VDA ISA (de 5.1 para 6.0.3)

© TECNOPLAST Ltda.. Todos os direitos reservados no caso de concessão de patente, modelo, documento ou desenho.
Uma cópia desse documento fora do controle do sistema de gestão de documentos estabelecido, é apenas para o propósito de informação e não é controlado.
A reprodução, distribuição e utilização deste documento, bem como a comunicação de seu conteúdo à terceiros sem autorização são proibidas.