Política de Segurança da Informação - PSI

PLASTICOMP IND COM COMP PLAST LTDA

Elaborado: Clayton Bernardi	Verificado: Cleonice Reis	Aprovado: Marco Vaiano

Política de Segurança da Informação da PLASTICOMP

A política de segurança da informação da PLASTICOMP, homologada pela diretoria, fornece as recomendações e diretrizes para garantir a continuidade dos negócios e minimizar os danos através da prevenção e diminuição do impacto de incidentes relacionados à segurança da informação.

Dentro dos objetivos e premissas desta política, a PLASTICOMP procura prestar seus serviços de forma consistente, com cada vez mais confiabilidade e eficiência e em total conformidade com os mais elevados padrões de segurança do mercado.

A segurança da informação é um ativo que, em nosso caso, é extremamente importante para nossos negócios, tem um alto valor para a nossa organização e consequentemente necessita ser adequadamente protegida.

A segurança da informação protege a informação de diversos tipos de ameaças minimizando os danos ao negócio, garantindo sua continuidade, maximizando o retorno dos investimentos e as oportunidades de negócio.

A segurança da informação na PLASTICOMP é caracterizada pela preservação da:

Integridade: Manutenção das informações como elas foram geradas.

Disponibilidade: Possibilidade de acesso contínuo, ininterrupto e constante das informações.

Confidencialidade: Manutenção do segredo, sigilo ou privacidade das informações.

Ambiente computacional:

O uso dos recursos computacionais da PLASTICOMP destina-se a atividades exclusivamente aprovadas pelo negócio, sendo obrigatório o uso apenas de softwares homologados e disponibilizados pela PLASTICOMP, instalados e gerenciados exclusivamente pelo departamento de T.I. ou sob sua supervisão e conhecimento.

Os usuários do ambiente computacional da PLASTICOMP devem informar todos os incidentes de segurança para a área de T.I. imediatamente após o seu conhecimento.

Acessos a DVDs, CDs, Pen-drive, Unidade em Massa do celular, HD externo etc., serão bloqueados. Em caso de necessidade de uso, será necessário preencher o formulário FO22015 – Controle de Acesso de Dispositivos, para permissão do acesso aos dispositivos, acima descritos. O documento será analisado pelo TI e pelo superior direto do colaborador.

Esta ação tem por objetivo prevenir a disseminação de vírus dentro do ambiente computacional da PLASTICOMP como resultado da manipulação de informações em suas atividades diárias.

As identificações de usuários para acesso aos recursos computacionais da PLASTICOMP são pessoais e intransferíveis, não devendo ser compartilhados em hipótese alguma.

É expressamente proibido ao funcionário utilizar-se de qualquer recurso ou tentativa para descoberta de contas e senhas de outros funcionários, bem como prover qualquer meio de burlar as regras de bloqueio de Internet, e-mail, acesso via IP a qualquer micro de usuário ou servidor, acesso a compartilhamentos sem prévia autorização do usuário ou qualquer outra forma de controle disponibilizada pela T.I. da PLASTICOMP.

TODAS AS ATIVIDADES DOS COLABORADORES DA PLASTICOMP EXECUTADAS ATRAVÉS DE SEUS RECURSOS COMPUTACIONAIS SÃO PASSÍVEIS DE MONITORAÇÃO PELO DEPARTAMENTO DE T.I.

Política de utilização dos recursos de TI:

O objetivo é disponibilizar aos funcionários, recursos de TI de alta qualidade e ao mesmo tempo desenvolver um comportamento extremamente ético e profissional, formalizar as regras de utilização que entendemos como violação ao uso dos serviços e recursos, aos quais são considerados proibidos.

Assim, para assegurar os altos padrões de qualidade na prestação desses serviços, faz-se
necessário a especificação de uma política de utilização.

Podemos definir como serviços e recursos os equipamentos utilizados pelos funcionários tais como: computadores (PC, notebooks), e-mails do domínio **plasticomp.com.br**, link de Internet, impressoras e telefonia móvel.

As normas descritas neste documento, não constituem uma relação exaustiva e poderão ser atualizadas com o tempo, sendo que qualquer modificação será notificada em tempo hábil para remodelação (se necessário) do ambiente de rede da PLASTICOMP.

Tais regras são fornecidas a título de orientação do funcionário. Em caso de dúvida sobre o que é considerado (violação), o usuário deverá enviar previamente um e-mail para **ti@plasticomp.com.br** visando esclarecimentos e segurança.

Nos termos da Política de utilização, a empresa procederá ao bloqueio do acesso ou cancelamento do usuário caso seja detectado uso inadequado, conforme estabelecido abaixo ou de forma prejudicial ao ambiente computacional da PLASTICOMP.

Atitudes que são consideradas violação à Política de Utilização dos recursos de TI foram divididas em tópicos:

1. **Utilização da rede**
2. **Utilização de e-mail**
3. **Utilização de acesso à internet**
4. **Utilização de impressoras**
5. **Utilização de microcomputadores**
6. **Monitoramento da aplicação da Política de utilização dos recursos de TI**
7. **Utilização da Rede Wifi da Sala de descanso**
8. **LGPD (Lei Geral de Proteção de Dados) – nº 13.7.09/2018**
9. **Responsabilidade Financeira**
10. **Concorrência Leal e ANTITRUSTE**
11. **Peças Falsificadas**
12. **Propriedade Intelectual**
13. **Compliance - Lei n° 12.846/13**
14. **Controles de Exportação e Sanções Econômicas**
15. **Denúncia e Proteção contra-retaliação**
16. **Punições**

1. Utilização da Rede

Esse tópico visa definir as normas de utilização da rede que engloba desde o acesso do usuário ao sistema, manutenção de arquivos no servidor e tentativas não autorizadas de acesso.

a) É proibida a tentativa de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta. Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes.

b) São proibidas as tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de invadir um servidor.

c) É proibido o uso de qualquer tipo de programa ou comando designado a interferir com sessão de usuários.

d) Antes de ausentar-se do seu local de trabalho, o usuário deverá bloquear seu microcomputador, evitando, desta maneira, o acesso por pessoas não autorizadas e efetuar a saída da rede ou sistemas em utilização de forma correta, conforme especificado pelo departamento de T.I.

e) Deverá ser efetuada a manutenção no diretório pessoal (incluindo os diretórios locais do microcomputador do usuário ou áreas compartilhadas na rede), evitando acúmulo de arquivos inúteis, que compromete o tamanho de disco do servidor.

f) É proibido material de natureza pornográfica e racista não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede.

g) É proibido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento dos sistemas.

As áreas de armazenamento de arquivos são designadas conforme abaixo:

Diretório Pessoal (área do usuário na rede), neste diretório deve ser gravado arquivos sigilosos apenas.

Diretório do setor em alguns casos poderá haver mais de um compartilhamento referente aos arquivos do departamento em qual o usuário faz parte.

Diretório público é de acesso a todos os usuários.

h) Qualquer pasta na rede, não deverá ser utilizada para armazenamento de arquivos que contenham assuntos pessoais, fotos particulares e quaisquer outros arquivos que não façam parte do uso profissional.

i) É obrigatório armazenar os arquivos referentes à empresa no servidor de arquivos (pasta do usuário na rede) para garantir o backup (cópia de segurança) dos mesmos.

j) Haverá limpeza sem prévio aviso dos arquivos armazenados na pasta do usuário na rede, que não sejam relativos ao negócio da PLASTICOMP, para que não haja acúmulo desnecessário de arquivos.

k) É proibida a instalação ou remoção de softwares que não forem devidamente acompanhadas pelo departamento de T.I., através de solicitação via chamado em helpdesk.plasticomp.com.br.

l) É proibida a abertura de computadores para qualquer tipo de reparo, caso seja necessário o reparo deverá ocorrer pelo departamento de T.I.

m) É proibida alteração de configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro.

2. Utilização de e-mail

Esse tópico visa definir as normas de utilização de e-mail que engloba desde o recebimento,
envio e gerenciamento das contas de e-mail.

a) É proibido o assédio, perturbação, linguagem inapropriada a qualquer pessoa.

b) É proibido o envio de e-mail a qualquer pessoa que não o deseje receber. Se o destinatário solicitar a interrupção de envio e-mails, o usuário deve acatar tal solicitação e não lhe enviar qualquer e-mail.

c) É proibido o envio de grande quantidade de mensagens de e-mail ou e-mails que não sejam de conteúdo profissional que estejam relacionados ao negócio da PLASTICOMP e que, de acordo com a capacidade técnica da rede, seja prejudicial ou gere reclamações de outros usuários.
Isso inclui qualquer tipo de mala direta, como, por exemplo, publicidade, comercial ou não, anúncios e informativos, propaganda política, fotos, arquivos PowerPoint ou filmes.

d) É proibido reenviar ou de qualquer forma propagar mensagens em cadeia ou "pirâmides" (mensagem para vários usuários), independentemente da vontade do destinatário de receber tais mensagens.

e) É proibido o envio de e-mail mal-intencionados ou sobrecarregar um usuário, site ou servidor com e-mail muito extenso ou numerosas partes de e-mail, bem como divulgar e-mails com conteúdo pornográfico ou obsceno.

f) Caso a empresa julgue necessário, haverá bloqueios.

1. De e-mail com arquivos anexos que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos.

2. De e-mail para destinatários ou domínios que comprometa o uso de banda ou perturbe o
bom andamento dos trabalhos.

g) É proibido forjar qualquer das informações do cabeçalho do remetente.

h) É obrigatória a limpeza da caixa de e-mail, evitando acúmulo de e-mails e arquivos inúteis. Tal ação poderá ser solicitada ao departamento de T.I que poderá auxiliar o usuário nesta tarefa.

i) É obrigatória a utilização de assinatura nos e-mails com o formato descrito abaixo, e para esta configuração deverá ser comunicado o departamento de T.I o qual auxiliará na configuração da assinatura:

3. Utilização de acesso à internet

Esse tópico visa definir as normas de utilização da Internet que engloba desde a navegação a sites, downloads e uploads de arquivos.

a) É proibido utilizar os recursos da empresa para fazer o download ou distribuição de software ou dados não legalizados.

b) É proibida a divulgação de informações confidenciais da empresa em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nesta política.

c) Poderá ser utilizada a Internet para atividades não relacionadas com os negócios durante o horário de almoço, desde que dentro das regras de uso definidas pelo departamento de T.I. Para este caso o colaborador deverá preencher o formulário FO 22015.

d) Funcionários com acesso à Internet não podem efetuar uploads (gravar arquivos em sites da internet) de qualquer software licenciado à empresa ou de dados de propriedade da empresa ou de seus clientes, sem expressa autorização do departamento de T.I.

e) Caso a empresa julgue necessário haverá bloqueios de acesso à arquivos que comprometam o uso de banda ou perturbe o bom andamento dos trabalhos.

f) Haverá monitoramento e geração de relatórios dos sites acessados por usuário e encaminhado ao gestor responsável.

g) É proibido o uso de softwares de comunicação instantânea, tais como Facebook, Whatsapp, Skype, Instagram, Linkedin, Youtube. Em caso de necessidade de acesso, o colaborador deverá preencher o formulário FO 22015.

h) É proibida a utilização de softwares P2P e Torrent tais como Kazaa, Morpheus, uTorrent e afins.

i) É proibida a utilização de sites e programas de música on-line, tais como, Rádio On-Line, Usina do som, Radio Terra, Spotify, Youtube, Deezer e afins.

j) É proibido o uso de redes sociais, como Facebook, Twitter, Badoo, Instagram, Linkedin e afins. Em caso de necessidade de acesso, o colaborador deverá preencher o formulário FO 22015.

k) É proibida a utilização de softwares de compartilhamento de arquivos, como Dropbox, Google Drive, e afins. Em caso de necessidade de acesso, o colaborador deverá preencher o formulário FO 22015.

l) É proibido o acesso a qualquer site com conteúdo pornográfico.

m) Não será permitido uso de sites que quebrem as regras de bloqueio ou controle de sites e e-mails na PLASTICOMP.

n) É de responsabilidade do departamento de T.I. a análise e liberação de sites para os usuários, podendo os mesmos ser bloqueados em caso de abuso.

4. Utilização de impressoras

Esse tópico visa definir as normas de utilização de impressoras disponíveis na rede.

a) Ao reimprimir, verifique na impressora se não há duplicidade de impressão, quando ocorrer qualquer problema no envio do documento.

b) Se a impressão saiu errada e o papel pode ser reaproveitado na sua próxima tentativa, recoloque-o na impressora, caso o papel não servir para impressão, transforme-o em rascunho, leve para sua mesa.

c) Não é permitido deixar impressões erradas na mesa das impressoras, na mesa das pessoas próximas a ela e tampouco sobre a impressora.

d) Se a impressora emitir alguma folha em branco recoloque-a na bandeja.

e) Se você notar que a quantidade de papel de alguma das impressoras estiver acabando faça a gentileza de reabastecê-la. Isso evita que você e outras pessoas tenham seus pedidos de impressão prejudicados e evita acúmulo de trabalhos na fila de impressão.

f) A utilização da impressora colorida é proibida, a liberação de acesso à mesma será efetuada pela direção.

g) A impressão do trabalho deverá ser somente para versão final dele, e não para testes ou rascunhos.

5. Utilização de microcomputadores

Esse tópico visa definir as normas de utilização de microcomputadores, notebooks, disponíveis na rede de dados.

a) É proibida a colocação de senhas no boot do micro, bem como em proteções de tela e área de trabalho. Serão aceitas exceções desde que solicitadas ao departamento de T.I. e informada a necessidade dela. Ressalta-se que a senha deverá ser de conhecimento da área de T.I. e estará proibida sua modificação sem aviso prévio.

b) É proibida a remoção ou instalação de quaisquer sistemas ou softwares sem previa autorização do departamento de T.I.

c) Os acessórios instalados nos computadores, tais como, mouses, teclados, monitor, devem ser conservados e no caso de quaisquer avarias, deve ser comunicado imediatamente ao departamento de T.I.

d) É de responsabilidade do usuário que utiliza notebook, cuidar e zelar pela integridade do equipamento. Ao receber o equipamento, o colaborador deverá assinar um termo de Responsabilidade de Utilização do Equipamento - FO 22016.

6. Monitoramento da aplicação da Política de utilização dos recursos de TI

Para garantir as regras mencionadas acima a PLASTICOMP se reserva no direito de:

a) Implantar softwares e sistemas que podem monitorar e gravar todos os usos de Internet e e-mail através da rede e das estações de trabalho da empresa.

b) Inspecionar qualquer arquivo armazenado na rede caso esteja no disco local da estação ou nas áreas privadas da rede, bem como e-mails.

c) É utilizada uma série de softwares e hardwares para proteger a rede interna e garantir a integridade dos dados e programas, bem como sistemas de controle de uso de internet e e-mail, antivírus, AntiSpam, firewall entre outros.

7. LGPD (Lei Geral de Proteção de Dados) – nº 13.7.09/2018

- Proteção e segurança de dados refere-se ao direito de um indivíduo de tomar suas próprias decisões sobre quem pode processar seus dados pessoais e para qual finalidade.

- Todos os colaboradores devem assinar aos termos da LGPD da PLASTICOMP (contrato de trabalho).

- A PLASTICOMP respeitará a decisão de cada colaborador referente aos seus dados.

- A PLASTICOMP cuidará dos dados dos colaboradores conforme a lei geral de proteção de dados número 13.7.09/2018.

- Os sistemas computacionais estão preparados e sempre atualizados conforme a lei geral de proteção de dados número 13.7.09/2018.

8. Responsabilidade Financeira

- Responsabilidade financeira refere-se à responsabilidade de uma empresa de registrar, manter e relatar com precisão a documentação comercial, incluindo, mas não limitado a contas financeiras, relatórios de qualidade, registros de tempo, relatórios de despesas e envios a clientes ou autoridades regulatórias, quando apropriado. Espera-se que os livros e registros sejam mantidos de acordo com a lei aplicável e os princípios contábeis geralmente aceitos. Fonte: Orientação Prática de Sustentabilidade Automotiva Global.

9. Concorrência Leal e ANTITRUSTE

- Competição justa e antitruste refere-se a empresas que mantêm padrões de negócios e concorrência justos, incluindo, mas não se limitando a, evitar práticas comerciais que restrinjam ilegalmente a concorrência, troca imprópria de informações competitivas e fixação de preços, manipulação de licitações ou alocação imprópria de mercado. É da responsabilidade primordial das grandes, médias e pequenas empresas cumprir as regras da concorrência. As empresas precisam estar cientes dos riscos de infringir as regras de concorrência e como desenvolver uma política/estratégia de conformidade que melhor se adapte às suas necessidades. Uma política/estratégia de compliance eficaz permite que uma empresa minimize o risco de envolvimento em infrações ao direito da concorrência e os custos resultantes de comportamento anticoncorrencial. Fonte: Orientação Prática de Sustentabilidade Automotiva Global e Comissão Europeia.

10. Peças Falsificadas

- Peças falsificadas refere-se à exigência de que as empresas desenvolvam, implementem e mantenham métodos e processos adequados aos seus produtos e serviços para minimizar o risco de introdução de peças e materiais falsificados em produtos entregues. As empresas também devem estabelecer processos eficazes para detectar peças e materiais falsificados e, se detectados, colocar os materiais em quarentena e notificar o cliente do fabricante de equipamento original (OEM) e/ou a aplicação da lei, conforme apropriado. Por fim, espera-se que as empresas confirmem que quaisquer vendas para clientes não OEM estão em conformidade com as leis locais e que os produtos vendidos serão usados de maneira legal. Fonte: Orientação Prática de Sustentabilidade Automotiva Global Propriedade intelectual refere-se a criações intelectuais, como invenções; obras literárias e artísticas; desenhos; e símbolos, nomes e imagens usados no comércio. É protegido por lei, por exemplo, por patentes, direitos autorais e marcas registradas, que permitem que as pessoas obtenham reconhecimento ou benefícios financeiros do que inventam ou criam. Fonte: Organização Mundial da Propriedade Intelectual.

11. Propriedade Intelectual

- Controles de exportação e sanções econômicas referem-se a restrições à exportação ou reexportação de bens, software, serviços e tecnologia, bem como às restrições aplicáveis ao comércio envolvendo determinados países, regiões, empresas ou entidades e indivíduos. Fonte: Orientação Prática de Sustentabilidade Automotiva Global Retaliação é definida como uma decisão e/ou ação administrativa adversa direta ou indireta que é ameaçada, recomendada ou tomada contra um indivíduo que relatou suspeita de irregularidade que implique um risco significativo ou cooperou com uma auditoria devidamente autorizada ou uma investigação de uma denúncia de irregularidade. Espera-se que as empresas estabeleçam processos (sistema de denúncia) que permitam que as preocupações sejam levantadas anonimamente com confidencialidade e sem retaliação. Fonte: Orientação Prática da OMS e da Sustentabilidade Automotiva Global.

12. Compliance - Lei n° 12.846/13

- O compliance tem o papel de criar mecanismos para evitar problemas maiores para a empresa no futuro, portanto todos os colaboradores devem participar do treinamento e esclarecimentos de Compliance, e assinar o Termo de Confidencialidade.

- É o dever de todos os colaboradores cumprirem aos termos da Compliance.

13. Controles de Exportação e Sanções Econômicas

- Controles de Exportação são regras específicas, impostas por determinados países e que restringem e regulam as operações de exportação de certos produtos para destinos específicos, sujeitando os exportadores destes países há limitações, restrições, licenças ou inclusive sanções em caso de inobservância destas regras. O tema é bastante complexo e, dentre os países que adotam os chamados Controles de Exportação, podemos citar Estados Unidos, países membros da União Europeia - como a Alemanha - e em geral, subsidiárias brasileiras de empresas sediadas nestes países deverão cumprir com as regras impostas.
- Benefícios: Estar em compliance com os procedimentos de conformidade internos (no caso de subsidiárias brasileiras de empresas sediadas em países que adotam Controles de Exportação), mitigando potenciais exposições e/ou sanções junto ao país de origem. Fonte: KPMG.

14. Denúncia e Proteção contra-retaliação

- O Decreto nº 10.890/2021, fica estabelecida a proteção contra retaliações a denunciantes, bem como medidas de reparação e incentivo à realização de denúncias, como: reforço ao papel da ouvidoria como centralizadora do recebimento de denúncias; criação de marcos processuais claros para fins de concessão de garantias contra retaliação; criação de procedimento centralizado na CGU para recebimento e apuração de denúncias de retaliação; possibilidade de a CGU adotar medidas acautelatórias e determinar medidas protetivas para fazer cessar a retaliação ao eventual risco ao denunciante.

15. Punições

O não cumprimento pelo colaborador, das normas ora estabelecidas neste Documento (Políticas de Segurança da Informação), seja isolada ou cumulativamente, poderá configurar infração cometida, as seguintes punições:

(A) COMUNICAÇÃO DE DESCUMPRIMENTO;

– Será encaminhado ao funcionário, por e-mail, comunicado informando o descumprimento da norma, com a indicação precisa da irregularidade praticada.

– Cópia desse comunicado permanecerá arquivada junto ao Departamento de gestão de pessoas, na respectiva pasta funcional do infrator.

(B) ADVERTÊNCIA OU SUSPENSÃO;

– A pena de advertência ou suspensão será aplicada, por escrito, somente nos casos de natureza grave ou na hipótese de reincidência de infrações de menor gravidade.

(C) DEMISSÃO POR JUSTA CAUSA;

– Nas hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho.

Fica desde já estabelecido que não haja progressividade como requisito para a configuração da dispensa por justa causa, podendo a Diretoria, no uso do poder diretivo e disciplinar que lhe é atribuído, aplicar a pena que entender devida quando configurada a falta grave.

Todos os colaboradores e gestores são responsáveis por:

- Aderir à política de Segurança da Informação da PLASTICOMP e as demais políticas estabelecidas.

Importante:

- Qualquer assunto não previsto nesta política deve ser submetido a análise do departamento de T. I e aprovado pelo departamento de recursos humanos e com aval da diretoria da PLASTICOMP.
- Os riscos provenientes da violação das informações devem ser gerenciados por todos, dentro de sua área de responsabilidade.
- Esta política será revisada anualmente, ou quando necessário, e efetuado o controle das revisões.
- Toda segurança das informações de dados e possíveis ataques cibernéticos, são protegidos por regras de firewall, utilizamos a marca: **Firewall Blockbit** – versão: **BLOCKBIT UTM 2.4.0 build 23040520** – modelo: **BBv-10.**
- Todas os computadores são protegidos com o **Antivirus Bitdefender** versão **7.9.5.324**, com atualizações diárias de engine, nesta ferramenta contamos com Antimalware/antivírus On-Access, Controle avançado de ameaças (ATC), Antiexploit, Mitigação de Ransomware, Firewall de cada computador individual secundário com monitoramento de alterações de processos, controle de conteúdo e análise de tráfego, Antiphishing, defesa contra ataques em rede, e analise de dispositivo externo via USB após inserção no computador.
- Utilizamos backup em nuvem, a solução utilizada é o **Acronis web**, em todos os servidores e máquinas prioridade, com 30 dias de backup salvo, e proteção contra Ransomware ativado.

- Todas as informações enviadas ao fornecedor (desenhos, normas, relatórios, amostras) são sigilosas e caracterizam segredo industrial, não podendo ser reproduzidas ou utilizadas para outros fins sem a devida autorização da CONTRATANTE, sob pena de medidas processuais na forma da lei.

HISTORICO

Data	Revisão	Motivo	Responsável
01/09/2023	01	Edição inicial	Clayton
20/02/2024	02	Alterado para atender TISAX	Clayton / Cleo