CMP - COMPANHIA METALGRAPHICA PAULISTA
DESDE 1924

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SUMÁRIO

1. VISÃO GERAL 3

2. OBJETIVO 3

2.1 MISSÃO DA ÁREA DE TECNOLOGIA DA INFORMAÇÃO 3
2.2 COMPROMETIMENTO 3

3. ABREVIATURAS E DESCRIÇÕES 3

4. DEFINIÇÕES DAS INFORMAÇÕES 4

4.1 INFORMAÇÃO PÚBLICA 4
4.2 INFORMAÇÃO INTERNA 4
4.3 INFORMAÇÃO CONFIDENCIAL 4
4.4 INFORMAÇÃO RESTRITA 4

5. CADASTRO E ACESSOS DOS USUÁRIOS 4

5.1 INCLUSÃO, ALTERAÇÃO E CANCELAMENTO DE ACESSO 4
5.2 PERMISSÕES E SENHAS 5
5.3 REVISÃO PERIÓDICA DE ACESSOS 6

6. COMPROMETIMENTO DOS USUÁRIOS 6

6.1 USO DO E-MAIL 6
6.2 USO DA INTERNET 7
6.3 USO DO ERP 7
6.4 PROGRAMAS NÃO AUTORIZADOS 8

7. PROTEÇÃO E ARMAZENAMENTO DE DADOS 8

7.1 USO DE ANTIVÍRUS 8
7.2 BACKUP NOS SERVIDORES 8
7.3 BACKUP NOS DESKTOPS 8
7.4 PROTEÇÃO E INTEGRIDADE DOS DADOS 8
7.5 COMPARTILHAMENTO DE DADOS 9
7.6 PROPRIEDADE INTELECTUAL 9
7.7 NOVOS SISTEMAS, APLICATIVOS E EQUIPAMENTOS 9

8. USO DE EQUIPAMENTOS DA ÁREA DE TI 9

8.1 EXCLUSIVIDADE DOS USUÁRIOS 9
8.2 EXCLUSIVIDADES DA ÁREA DE TI 10

9. INDICADORES 10

10. RESPONSABILIDADES 10

11. PENALIDADES 11

12. REVISÃO DA POLÍTICA 11

13. DOCUMENTOS RELACIONADOS 11

14. ANEXO – TERMO DE ACEITE 12

1. VISÃO GERAL

A Política de Segurança da Informação da CMP COMPANHIA METALGRAPHICA PAULISTA, aplica-se a todos os colaboradores, fornecedores e consultores, que utilizem o ambiente de processamento ou acesso as informações da companhia. Qualquer usuário dos sistemas da CMP tem a responsabilidade de proteger a integridade das informações e dos equipamentos de informática.

Violações desta Política:

- Expor a CMP a uma perda monetária por meio do comprometimento da segurança dos dados, de informações ou perda de equipamento.
- Revelar dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.
- Usar os dados com propósitos que violem as leis, regulamentos ou quaisquer outros dispositivos legais.

2. OBJETIVO

Assegurar que somente os usuários autorizados tenham acesso as informações da CMP, estabelecendo critérios para o controle desses acessos.

2.1 Missão da área de Tecnologia da Informação

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização das atividades da CMP. Gerir o processo de segurança e proteger as informações da organização, incentivando, coordenando, desenvolvendo e implementando ações para esta finalidade.

2.2 Comprometimento

Considerar as informações sigilosas como recursos críticos para a realização e continuidade do negócio, que é de importância da CMP e devem ser tratadas profissionalmente.

3. ABREVIATURAS E DESCRIÇÕES

- TST Tribunal Superior do Trabalho.
- TRT Tribunal Regional do Trabalho.
- NAS *Network Attached Storage* (Armazenamento Anexado à Rede).

- ERP *Enterprise Resource Planning* (Sistema integrado de gestão empresarial).

4. DEFINIÇÕES DAS INFORMAÇÕES

4.1 Informação Pública

É toda informação que pode ser acessada pelos usuários da CMP, clientes, fornecedores, prestadores de serviços e público em geral.

4.2 Informação Interna

É toda informação que pode ser acessada por colaboradores da organização. São informações que possuem um grau de confidencialidade que podem comprometer a imagem da CMP.

4.3 Informação Confidencial

É toda informação que pode ser acessada pelos usuários e parceiros da companhia. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) para ambas as partes.

4.4 Informação Restrita

É toda informação que pode ser acessada somente pelos usuários da CMP indicado pelo nome ou pela área a que pertence. A divulgação não autorizada de informações pode causar danos ao negócio ou comprometer a estratégia da companhia.

Os gestores devem orientar seus colaboradores a não circularem mídias, divulgarem informações confidenciais ou restritas, como também não deixarem relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar documentos confidenciais ou restritos sobre as mesas.

5. CADASTRO E ACESSOS DOS USUÁRIOS

5.1 Inclusão, Alteração e Cancelamento de Acesso

A área de Recursos Humanos da CMP deverá informar a área de TI, qualquer movimentação de temporários, estagiários, colaboradores, para que os mesmos possam ser cadastrados ou excluídos nos sistemas e ferramentas da CMP.

No caso de contratação de consultores, os gestores dos contratados deverão informar à área de TI a necessidade de acesso à sistemas.

Isto inclui o fornecimento de senha *password* e registro de nome como usuário no sistema *user-id*, realizado pela área de TI.

O gestor do contratado deve comunicar a área de TI sobre as rotinas que o contratado terá permissão de acesso. No caso de temporários, estagiários e consultores deverá ser informado o tempo de prestação de serviço para a CMP, e na data de seu desligamento possam também ser encerradas as atividades relacionadas a permissão de seu acesso aos sistemas e ferramentas. No caso de demissão, a área de Recursos Humanos deverá comunicar imediatamente a área de TI, para que desligado seja excluído dos sistemas e solicitada a devolução de equipamentos que foram fornecidos.

No caso de alterações nas atribuições laborais, como por exemplo, transferência para novo cargo ou função que tornem o acesso anterior desnecessário ou incompatível para o cumprimento de suas atividades, devem ser comunicadas à área de TI.

5.2 Permissões e Senhas

Para acessar os dados da rede da CMP, o usuário deverá possuir um login e senha previamente fornecido pela área de TI.

O gestor do usuário deverá fornecer os dados referente os tipos de rotinas, programas e permissões de acesso, através da abertura de chamado para a área de TI através do link http://srvcmp02:8080/portal.

Após o cadastramento do contratado, a área de TI informará a primeira senha de acesso, que obrigatoriamente deverá ser alterada pelo usuário. No período de 50 dias a senha da rede expirará e o usuário deverá atualizá-la.

A área de TI estabeleceu que, para cada sistema é exigido haja um critério mínimo para criação ou alteração das senhas, contendo no mínimo de 6 caracteres devendo ter letras e números e não podendo repetir as 3 últimas senhas.

O acesso de usuários externos deverá ser bloqueado assim que concluído o trabalho, havendo necessidade de novo acesso, deverá ser solicitado o desbloqueio para a área de TI.

A área de TI reserva-se no direito de não conceder ou revogar permissões sem prévio aviso caso avalie algum risco para CMP.

5.3 Revisão Periódica de Acessos

Os acessos às informações são revisados periodicamente, com o objetivo de assegurar a pertinência e a conformidade dos acessos. As revisões são realizadas uma vez por ano, podendo ocorrer em periodicidade menor. O resultado da revisão pode ser enviado para a anuência dos gestores, mediante solicitação.

6. COMPROMETIMENTO DOS USUÁRIOS

6.1 Uso do E-mail

O e-mail fornecido ao usuário é um instrumento de comunicação interno e externo para a execução das atividades da companhia. As mensagens devem ser escritas de forma profissional.

É proibido o envio de mensagens com os seguintes conteúdos:

- Que tenham declarações difamatórias e linguagem ofensiva;
- Que possam trazer prejuízos a outras pessoas;
- Que sejam hostis e inúteis;
- Que comprometam a imagem da CMP;
- Que comprometam os princípios éticos da CMP;
- Que infrinjam as legislações vigentes;
- Que sejam relativas a correntes ou conteúdos equivalentes;
- Que possam prejudicar a imagem de outras empresas.

Não é permitido o uso de e-mails gratuitos liberados em alguns sites (ex.: hotmail, gmail, yahoo, entre outros), a área de TI poderá bloquear o recebimento destes e-mails, evitando a invasão de vírus nos microcomputadores.

O TST reconhece o direito das organizações em obter provas através de recursos para rastreamento dos e-mails enviados, recebidos ou armazenados pelos usuários, havendo a possibilidade de rescisão do contrato de trabalho por Justa Causa.

É cedido ao empregador a permissão de exercer o controle do conteúdo das mensagens que trafegam pelo seu sistema de informática, com a finalidade de evitar riscos de prejuízos à organização;

O e-mail fornecido pela companhia tem natureza jurídica, equivalente a uma ferramenta de trabalho. Dessa forma, este recurso deverá ser destinado exclusivamente para o desenvolvimento das atividades profissionais.

De acordo com o TRT a organização poderá rastrear todos os endereços eletrônicos, pois os e-mails são disponibilizados para fins profissionais.

6.2 Uso da Internet

O acesso à Internet será autorizado para os usuários que desempenham atividades na CMP. Somente é permitido o acesso às informações com conteúdo profissional e para o negócio.

O uso da Internet é monitorado pela área de TI, através de “logs” que informam o usuário, o tempo e a página acessada.

Os gestores dos colaboradores definirão a permissão para o uso da internet, com base nas recomendações da Gerência de TI.

Não é permitido instalar programas da Internet nos microcomputadores sem a autorização da área de TI. Os usuários não devem infringir direitos autorais de marcas, licenças de uso ou patentes de terceiros. É proibido transferir informações, efetuar *download*, copiar ou qualquer outra ação em sites dos tipos:

- De conteúdo pornográfico ou relacionados a sexo;
- Que defendam atividades ilegais;
- Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
- Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios da CMP;
- Que possibilitem a distribuição de informações de nível “Confidencial”;
- Que permitam a transferência, *downloads* de arquivos ou programas ilegais;
- Sites de Jogos e afins;
- Quaisquer Sites ou Programas para investimentos e operações no mercado financeiro (ex.: Bolsa de Valores, Day Trade, Criptomoedas, Forex, entre outros da mesma categoria).

6.3 Uso do ERP

O acesso ao Sistema ERP será autorizado pela área de TI somente para os usuários que desempenham atividades de apoio no gerenciamento das informações e perfil de acesso específico para a funcionalidade exercida.

As atualizações das versões e releases devem ser programadas pela área de TI com anuência das áreas integradas no sistema.

Os usuários devem seguir as orientações e treinamentos estipulados pela CMP assegurando a integridade dos dados.

6.4 Programas Não Autorizados

Em cumprimento aos direitos autorais, a CMP permite o uso somente de programas licenciados.

Somente colaboradores da equipe da área de TI tem a permissão para instalação de programas autorizados. Periodicamente, área de TI deve realizar verificações no banco de dados dos servidores ou nos computadores dos usuários, visando assegurar a correta aplicação das diretrizes desta Política. Caso sejam identificados programas não autorizados, serão removidos e informados aos gestores, estando sujeitos as penalidades previstas nesta Política.

7. PROTEÇÃO E ARMAZENAMENTO DE DADOS

7.1 Uso de Antivírus

Todos os microcomputadores da CMP devem ter programa antivírus, devendo ser atualizado automaticamente pela área de TI. Arquivos obtidos de forma externa ou através da Internet, serão verificados por Antivírus. O usuário não deve desabilitar o antivírus instalado nos microcomputadores.

7.2 Backup nos Servidores

O *backup* (cópia de segurança dos dados) é realizado diariamente, abrangendo os arquivos localizados nos servidores de dados em nuvem.

Os dados do *backup* são armazenados em unidades de Alta Capacidade (NAS) internamente e em *Cloud Backup*, permitindo assim um *disaster recovery* estando prontamente disponíveis para serem restaurados.

7.3 Backup nos Desktops

É responsabilidade dos usuários efetuarem *backup* (cópias de segurança) de dados, arquivos ou documentos nas áreas de trabalho.

7.4 Proteção e Integridade dos Dados

O gerenciamento dos bancos de dados é de responsabilidade da área de TI, assim como a manutenção, alteração e atualização de equipamentos e programas.

Demais orientações quanto as práticas e processos, deverão ser observadas na Política de Proteção de Dados.

7.5 Compartilhamento de Dados

Não são permitidos na empresa o compartilhamento de dispositivos móveis tais como pen-drivers e outros nos microcomputadores.
A utilização de impressoras deve estar sujeita as permissões de acesso concedido pela área de TI.

7.6 Propriedade Intelectual

É de propriedade da CMP, todos os *designs*, criações ou procedimentos desenvolvidos por qualquer colaborador durante o vínculo empregatício.

7.7 Novos Sistemas, Aplicativos e Equipamentos

A área de TI é responsável pela aplicação da Política da CMP em relação a definição de compra e substituição de *software* e *hardware*. Qualquer necessidade de novos programas ou equipamentos de informática deverá ser analisada pela área de TI. Não é permitida a compra ou o desenvolvimento de *softwares* ou *hardwares* diretamente pelos usuários.

8. USO DE EQUIPAMENTOS DA ÁREA DE TI

8.1 Exclusividade dos Usuários

Os usuários que tiverem permissão de uso de computadores (microcomputador, laptop ou notebook), celular, ou qualquer outro equipamento computacional de propriedade da CMP, devem estar cientes de que:

(a) A proteção do recurso computacional de uso individual é de responsabilidade do usuário.

(b) É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.

(c) O usuário não deve alterar a configuração do equipamento.

Alguns cuidados que devem ser observados fora do trabalho:

- Mantenha o equipamento sempre em seus cuidados;
- Atenção à proteção dos equipamentos em hall de hotéis, aeroportos, aviões, táxis entre outros;
- Sempre que necessário o transporte de equipamentos em veículos, coloque-os no porta-malas ou lugar não visível;

Em caso de furto:

- Registre a ocorrência em uma delegacia de Polícia ou pela internet e envie uma cópia para a área TI.
- Comunique a ocorrência ao seu gestor.

Não é permitida a saída com qualquer equipamento fixo sem autorização da área de TI e gestores.

8.2 Exclusividades da Área de TI

Toda movimentação de equipamento é de responsabilidade da área de TI, como por exemplo, microcomputadores, impressoras entre outros.

É de responsabilidade da área de TI o controle, concessão e a aplicação de restrições em relação aos ramais telefônicos e celulares da CMP, de acordo com as definições dos gestores.

9. INDICADORES

Bimestralmente a área de TI gera indicadores para monitoramento e acompanhamento das atividades como:

Chamados técnicos

a) Número total de chamados
b) Total de horas de chamados
c) Chamados por categoria

Portfólio de projetos

a) Total de projetos por Status
b) Total de horas de projetos
c) Previsões de investimos
d) Esses indicadores são reportados para diretoria e Vice Presidência.

10. RESPONSABILIDADES

- **Área de TI**

Orientar os usuários quanto as diretrizes desta Política e obter as devidas assinaturas de concordância.

Realizar auditorias periódicas do acesso dos usuários às informações, verificando:

- Que tipo de informação o usuário pode acessar;
- Quem está autorizado a acessar determinada rotina ou informação;

- Quem acessou determinada rotina e informação;
- Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;
- Que informação ou rotina o usuário acessou;
- Quem tentou acessar qualquer rotina ou informação sem estar autorizado.

A área de TI poderá conceder ou revogar permissões sem prévio aviso, caso avalie algum risco para CMP.

- **Gestores**

Estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios ou mídias) geradas pela área.

Definir os acessos de seus colaboradores e consultores aos sistemas e informações da CMP, cabendo verificar se os usuários estão acessando as rotinas compatíveis com as suas respectivas funções e conservando adequadamente os equipamentos.

- **Área de Recursos Humanos**

Informar a área de TI qualquer movimentação de colaboradores, temporários ou estagiários após formalização.

11. PENALIDADES

O não cumprimento desta Política implica em falta grave e poderá resultar em Advertência Formal, Suspensão, Rescisão do Contrato de Trabalho, processo civil/criminal ou outra ação disciplinar.

12. REVISÃO DA POLÍTICA

Aprovada pela Alta Administração e implementado no dia 03 de junho de 2022.

Este documento será revisado sempre que necessário.

13. DOCUMENTOS RELACIONADOS

- Código de Conduta e Ética para Colaboradores.

- ISO 27001 Gestão de Segurança da Informação (Em caráter consultivo)

- Política de Proteção de Dados.

14. ANEXO – TERMO DE ACEITE

Eu,_____, da área _____, portador do nº de RE_____, declaro que estou de acordo com a Política de Segurança da Informação da CMP COMPANHIA METALGRAPHICA PAULISTA, e me comprometo a seguir suas diretrizes.

Local: _____UF: _____, Data: _____ de _____ de 20____.

Assinatura: _____.

	CMP - COMPANHIA METALGRAPHICA PAULISTA		
Área	**Título**	**Identificação**	**Revisão**
TECNOLOGIA DA INFORMAÇÃO	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	POL.TI.02	00.2022
Elaborado / Revisado por: Georgeo Nocera – Gerente de Tecnologia da Informação		**Aprovado por:** Jose Vilella de Andrade – Diretor Vice-Presidente	

HISTÓRICO		
Revisão	**Aprovação**	**Alteração**
00.2022	03/06/2022	Emissão Inicial