



GEWISS PORTUGAL  
INDÚSTRIA DEL MATERIAL ELÉCTRICO,  
UNIPessoal, LDA

CÓDIGO DE CONDUTA TI

## ÍNDICE

INTRODUÇÃO .....	3
1. DEFINIÇÃO .....	3
2. SISTEMA DE INFORMAÇÃO DA EMPRESA – REGRAS GERAIS .....	3
3. USO DE EQUIPAMENTOS DE TECNOLOGIAS DE INFORMAÇÃO .....	4
4. SENHAS DE ACESSO (PALAVRAS-PASSE) .....	5
5. USO DA REDE DA EMPRESA .....	5
6. USO DA REDE INTERNET E SERVIÇOS RELACIONADOS .....	6
7. USO DE CORREIO ELECTRÓNICO .....	6
8. CONTROLO .....	7
9. NÃO OBSERVÂNCIA DAS INSTRUÇÕES E SANÇÕES.....	8

## INTRODUÇÃO

A difusão progressiva das novas tecnologias de informação pode expor a GEWISS tanto a riscos de propriedade como a riscos penais, criando enquanto isso problemas de imagem e de segurança a nível "corporate", caso o equipamento de tecnologias de informação seja usado de forma incorreta ou para crimes. A importância crescente de informações confidenciais dentro dos activos da empresa e as decorrentes da vantagem competitiva da empresa têm feito com que a mesma se tenha dotado com as medidas de protecção adequadas destinadas a prevenir a difusão de dados e informações confidenciais que poderiam causar tanto responsabilidades civis como penais para a pessoa que viole a confidencialidade da empresa.

Por isso, considera-se oportuno o desejo da empresa em proteger a sua informação confidencial equipando-se com medidas efectivas (por exemplo com medidas de segurança) para a protecção da informação de natureza confidencial.

Além disso, referindo-se ao tratamento de dados pessoais, a GEWISS deu explicações adequadas e instruções a todos os "utilizadores da empresa", que, trabalhando com ferramentas de tecnologias de informação, estejam interessados nas medidas anteriormente referidas.

Considerando-se que o uso de informações e recursos telemáticos do tipo "corporate" deve ser sempre conduzido com cuidado e com princípios de equidade, atitudes que devem sempre ser tomadas durante o trabalho, é útil adoptar mais regras comportamentais internas no âmbito da gestão de informação, direccionadas a evitar comportamentos errados por desconhecimento e/ou incorrectos.

## 1. DEFINIÇÃO

Para efeitos do presente Código de Conduta de TI, o significado fornecido para cada um dos termos e expressões listados abaixo é válido para o termo/expressão da seguinte forma:

- "CÓDIGO DE CONDUTA TI": este documento;
- "EMPRESA": a empresa GEWISS PORTUGAL;
- "EMPRESA ASSOCIADA": a empresa GEWISS S.p.A.;
- "RESPONSÁVEL DE SEGURANÇA": pessoa encarregada pela GEWISS S.p.A. de gerir dentro da EMPRESA os dados pessoais, gerir a transferência e comunicação de dados, assim como, gerir as medidas de segurança relacionadas, de acordo com a legislação em vigor;
- "EQUIPAMENTO DE TECNOLOGIAS DE INFORMAÇÃO": qualquer equipamento diferente de papel usado por qualquer utilizador da empresa para desempenhar as suas tarefas, entre as quais, a título exemplificativo, se considera computadores pessoais, tanto os fixos como os portáteis, PDA ou "smartphones", telefones fixos e móveis;
- "SISTEMA DE INFORMAÇÃO": recursos, dados, aplicativos e programas instalados no equipamento de TI e/ou dispositivos de armazenamento de dados;
- "UTILIZADOR DA EMPRESA": qualquer utilizador, mesmo que não seja um funcionário da EMPRESA, a quem foi dado um ou mais EQUIPAMENTOS DE TECNOLOGIAS DE INFORMAÇÃO e/ou foi dado acesso para usar o sistema de informação da empresa.

## 2. SISTEMA DE INFORMAÇÃO DA EMPRESA – REGRAS GERAIS

Todos os EQUIPAMENTOS DE TECNOLOGIAS DE INFORMAÇÃO, os respectivos programas e/ou todas as aplicações, disponibilizados aos UTILIZADORES DA EMPRESA são consideradas ferramentas de trabalho.

Consequentemente:

- 2.1 essas ferramentas devem ser mantidas de forma adequada;
- 2.2 essas ferramentas só podem ser utilizadas para fins profissionais (obviamente relacionados com seus deveres) e não para fins pessoais, muito menos para crimes;
- 2.3 é proibido emprestar ou dar a terceiros qualquer EQUIPAMENTO DE TECNOLOGIAS DE INFORMAÇÃO;
- 2.4 é proibido remover as marcas de identificação do EQUIPAMENTO DE TECNOLOGIAS DE INFORMAÇÃO;
- 2.5 qualquer roubo, dano ou perda de equipamento informático deve ser imediatamente comunicado à

EMPRESA e ao próprio Departamento. Além disso, em caso do computador ser roubado ou perdido, a pessoa envolvida, ou a pessoa a quem foi cedido qualquer EQUIPAMENTO DE TECNOLOGIAS DE INFORMAÇÃO, deve enviar à EMPRESA a cópia do relatório original apresentado à Autoridade de Segurança Pública no prazo de 24 horas a partir da ocorrência dos factos;

- 2.6 é proibida a introdução e/ou retenção dentro da EMPRESA, por meio de qualquer capacidade e por qualquer razão, (por meio de qualquer ferramenta informática, hardware e papel), todo o tipo de material confidencial ou de tecnologias de informação de terceiros e/ou documentos, sem a autorização prévia do proprietário. Entende-se que, em caso de violação, a responsabilidade civil e penal pessoal do empregado, bem como as sanções disciplinares da EMPRESA devam ser aplicadas;
- 2.7 é proibido trazer para fora da empresa e/ou transmitir ficheiros, documentos, desenhos, projectos ou quaisquer outros documentos confidenciais da EMPRESA, por meio de computador, hardware e de papel, se não para fins estritamente respeitantes à execução das suas tarefas e, em qualquer caso, sujeita a autorização do correspondente Responsável do Departamento;
- 2.8 é absolutamente proibido partilhar nas áreas comuns ficheiro (como, por exemplo, em workspace/rede local, entre outros), ou, em qualquer caso, passar documentos e informações dentro da empresa que não estejam ligados ao remetente ou às actividades profissionais do destinatário, usando qualquer ferramenta de TI, hardware e papel;
- 2.9 é proibido o registo de documentos ofensivos e/ou discriminativos quanto ao sexo, língua, religião, raça, origem étnica, opinião e filiação sindical ou política no SISTEMA INFORMÁTICO da empresa;
- 2.10 em caso de cessação da relação laboral, seja ela por qual motivo for, os UTILIZADORES DA EMPRESA têm que devolver à EMPRESA todos os EQUIPAMENTOS INFORMÁTICOS e as ferramentas de trabalho que lhes tenham sido atribuídas em estado de uso. A eliminação de todos os ficheiros de dados gravados no EQUIPAMENTO INFORMÁTICO e nas ferramentas de trabalho é sempre executada na presença da EMPRESA, pela pessoa responsável;
- 2.11 a qualquer momento, a EMPRESA tem o direito de usar de forma diferente os EQUIPAMENTOS INFORMÁTICOS cedidos aos UTILIZADORES DA EMPRESA, solicitar a sua devolução imediata e/ou de os examinar, de forma a verificar a sua correcta utilização.

### 3. USO DE EQUIPAMENTOS DE TECNOLOGIAS DE INFORMAÇÃO

Para os fins acima mencionados, cada acto ou atitude que contrasta com as instruções anteriores é proibido. Alguns exemplos são dados abaixo, de forma indicativa:

- 3.1 para evitar o perigo de um vírus informático e de danos para a estabilidade do computador pessoal e das suas aplicações, os utilizadores estão apenas autorizados a instalar programas externos quando expressamente autorizado pela EMPRESA.
- 3.2 é proibida a instalação e a utilização de programas que não tenham sido autorizados pela EMPRESA, que dará a sua autorização se forem cumpridas as obrigações legislativas sobre a protecção legal de software e de direitos de autor.
- 3.3 é proibido modificar as configurações definidas nos EQUIPAMENTOS INFORMÁTICOS, sem autorização prévia da EMPRESA.
- 3.4 é proibido instalar e/ou conectar aos EQUIPAMENTOS INFORMÁTICOS quaisquer dispositivos periféricos adicionais que não tenham sido autorizados pela EMPRESA.
- 3.5 nos computadores pessoais equipados com dispositivos de áudio e/ou CD/DVD, é proibido ouvir ficheiros de áudio ou de música ou assistir a vídeos e filmes, se não relacionadas com o trabalho.
- 3.6 os utilizadores não estão autorizados a deixar os seus próprios EQUIPAMENTOS INFORMÁTICOS abandonados e/ou acessíveis a outros. Durante longos períodos de ausência deve ser activada a função de bloqueio de PC/equipamento.
- 3.7 é proibido deixar qualquer EQUIPAMENTO INFORMÁTICO portátil (computador portátil, PDA, smartphones, vídeo-projectores, telemóveis, entre outros) abandonados e/ou acessíveis a outros durante transferências (ex: parques de estacionamento, etc), viagens de negócios (ex: aeroportos, estações, etc), ou, em caso de ausência da EMPRESA (férias, no fim de semana, durante a noite).

#### 4. SENHAS DE ACESSO (PALAVRAS-PASSE)

- 4.1 As senhas de acesso que dão acesso à rede da empresa devem ser mantidas em segredo; conseqüentemente, todos têm que manter o sigilo das suas senhas de acesso.
- 4.2 As senhas de acesso não podem ser transferidas a terceiros. Etiquetas e/ou bilhetes que indiquem a identificação de utilizador ou a senha de acesso não podem ser expostas no computador.
- 4.3 As senhas de acesso devem conter 8 caracteres, não devem conter referências ao utilizador, têm que ser modificadas pelo próprio utilizador no primeiro acesso e têm que ser alteradas pelo menos de três em três meses.
- 4.4 É absolutamente proibida a utilização de senhas de acesso pertencentes a outros UTILIZADORES DA EMPRESA, mesmo que o acesso seja para proteger as próprias áreas do UTILIZADOR DA EMPRESA, excepto quando expressamente autorizado pelo responsável de UTILIZADORES DA EMPRESA e pelo RESPONSÁVEL DE SEGURANÇA.

#### 5. USO DA REDE DA EMPRESA

- 5.1 As unidades de rede e área de espaço de trabalho “workspace” são áreas que contêm informações compartilhadas de cariz estritamente profissional e não podem ser usadas para fins diferentes.  
  
Os modos operacionais para ter correctamente acesso aos dados electrónicos são regulados em detalhe em procedimentos/instruções de trabalho adoptados pela EMPRESA e pela EMPRESA ASSOCIADA, que são considerados parte integrante deste documento.  
  
A EMPRESA tem o direito de modificar as autorizações de acesso à rede da empresa e às aplicações relevantes, caso a integridade de todos os dados de informação da empresa sejam colocados em risco, mesmo se apenas potencialmente.
- 5.2 Qualquer ficheiro que não esteja relacionado com o trabalho do utilizador não pode ser colocado, nem mesmo por períodos curtos, no SISTEMA DE INFORMAÇÕES DA EMPRESA e no EQUIPAMENTO DE TECNOLOGIA DE INFORMAÇÃO.
- 5.3 O acesso de cada funcionário a qualquer recurso do SISTEMA DE INFORMAÇÃO da empresa (pastas na rede da empresa, áreas comuns, etc) tem que ser autorizado pelo correspondente responsável da função das tarefas atribuídas a cada colaborador; assim, cada UTILIZADOR DA EMPRESA deve, portanto, usar a rede da empresa para fins estritamente ligados ao desempenho das suas tarefas e de acordo com o previsto na correspondente autorização.
- 5.4 Cada UTILIZADOR DA EMPRESA tem de proteger a confidencialidade dos dados que esteja a processar, prestando particular atenção aos dados compartilhados e qualquer cópia em papel dos dados electrónicos e remove-los de forma definitiva, quando esses dados já não sejam necessários; em particular, é altamente recomendável, proteger com senha de acesso todos os documentos que sejam temporariamente arquivados naquelas áreas comuns que todos os UTILIZADORES DA EMPRESA podem ter acesso.
- 5.5 A qualquer momento, a EMPRESA tem o direito de remover qualquer ficheiro ou aplicativo considerado perigoso para a segurança do sistema e qualquer ficheiro ou aplicativo adquirido e/ou instalado que viole o presente CÓDIGO DE CONDUTA DE TI; em especial, a EMPRESA tem o direito de eliminar os dados guardados em áreas compartilhadas, comuns a todos os UTILIZADORES DA EMPRESA dentro de 24 horas a partir do momento da sua gravação.
- 5.6 É proibida a instalação e o uso de software e/ou hardware para interceptar conversações (em qualquer forma que seja, uma conversa telefónica, sms, correio electrónico, etc) e falsificar, alterar ou suprimir o conteúdo de comunicações e/ou documentos TI da empresa.
- 5.7 É proibido conectar à rede da empresa qualquer PC ou outro equipamento informático não pertencente à EMPRESA, excepto que seja expressamente autorizado pela EMPRESA.

## 6. USO DA REDE INTERNET E SERVIÇOS RELACIONADOS

A EMPRESA garante o acesso à internet apenas para os UTILIZADORES DA EMPRESA que precisam do acesso a partir de seu próprio local de trabalho. A conexão com a internet deve ser mantida durante o tempo estritamente necessário para a realização dessas actividades ligadas ao uso da internet. Por isso:

- 6.1 é proibido de navegar em páginas não relacionadas com o trabalho;
- 6.2 é proibido transferir e salvar documentos não autorizados e documentos insultantes/ discriminativos quanto ao sexo, língua, religião, raça, origem étnica, opinião e de associação sindical e /ou política;
- 6.3 é proibido executar qualquer transacção bancária incluindo operações de “homebanking”, compras on-line e operações similares, excepto nos casos previstos pelos procedimentos da empresa que regem as regras de compra da empresa;
- 6.4 é proibido o transferir de sites da internet qualquer tipo de software não autorizado expressamente pela EMPRESA;
- 6.5 é proibido qualquer registo em sites cujo seu conteúdo não esteja relacionado com o próprio trabalho;
- 6.6 é proibido usar e consultar, por motivos particulares, serviços tais como fóruns, redes sociais, linhas de bate-papo (chats), grupos de novidades, quadros de aviso electrónicos ou similares e registos em livros de visitantes, mesmo usando uma alcunha;
- 6.7 é proibido tornar-se membro de fóruns, redes de bate-papo “chats”, blogs, grupos de novidades, quadros de aviso electrónicos ou similares, usando para o efeito o correio electrónico da empresa, excepto quando expressa e previamente autorizado pelo correspondente Responsável do Departamento. Em qualquer caso, todos são directamente responsáveis pelo uso correcto e legítimo do endereço de correio electrónico da empresa, bem como pelo conteúdo das declarações e das informações transmitidas;
- 6.8 a única conexão à internet autorizada é através da rede da empresa; outras conexões diferentes, por exemplo os que usam linhas telefónicas da empresa, não são autorizadas para esse fim;
- 6.9 a qualquer momento, a EMPRESA e a EMPRESA ASSOCIADA têm o direito de activar alguns filtros na navegação web da internet, bloqueando o acesso a “sites” não relacionados com a actividade de trabalho, para páginas perigosas ou páginas que poderiam potencialmente causar uma violação deste Código e procedimentos/instruções relacionadas adoptadas pela EMPRESA e pela EMPRESA ASSOCIADA, de acordo com a legislação em vigor.

## 7. ELECTRÓNICO

A empresa fornece, na medida da necessidade dos utilizadores da empresa, uma caixa de correio electrónico pessoal, que é inequivocamente atribuída. Também a caixa de correio electrónico é uma ferramenta de trabalho disponível para realizar as actividades ligadas às tarefas atribuídas, portanto, o endereço atribuído aos utilizadores da empresa é pessoal, mas não privado. Cada um é directamente responsável, diante da disciplina e da lei, pelo conteúdo da sua própria caixa de correio electrónico e pelas mensagens enviadas.

O uso de caixas de correio electrónico tem que ser compatível com os procedimentos internos e com as seguintes regras:

- 7.1 É proibido usar as caixas de correio electrónico, tanto as internas como externas para fins não relacionados com o próprio trabalho;
- 7.2 É proibido enviar ou guardar qualquer mensagem interna ou externa de natureza ofensiva e/ou discriminativa quanto ao sexo, língua, raça, de origem étnica, opinião, e de filiação sindical ou política;
- 7.3 Todas as mensagens externas, ambas enviadas ou recebidas, podem ser compartilhadas e vistas dentro da EMPRESA;
- 7.4 É proibido o uso do correio electrónico pertencente a outros UTILIZADORES DA EMPRESA para enviar mensagens no próprio nome ou em nome desse utilizador excepto quando existe autorização explícita do correspondente. Em caso de ausência programada do trabalhador é altamente recomendado ao UTILIZADOR DA EMPRESA para partilhar a sua caixa de correio electrónico, activando a resposta automática (o chamado aviso “fora do escritório”) com a possibilidade de indicação de uma pessoa

de referência para ser contactada em caso de assuntos urgentes e suas referências de correio electrónico e/ou de telefone. A mensagem "fora do escritório" deve ser activada tanto para remetentes internos como para os externos;

- 7.5 O acesso às caixas de correio electrónico de um UTILIZADOR DA EMPRESA ausente e o conhecimento de todas as mensagens necessárias pode ser possível, em conformidade com o que estiver previsto na legislação em vigor e de acordo com as instruções fornecidas no procedimento específico adoptado pela EMPRESA para o efeito;
- 7.6 Caixas de correio electrónico são criadas e atribuídas sem qualquer configuração para partilha e/ou regras. Cada UTILIZADOR DA EMPRESA é, portanto, responsável por qualquer partilha possível e/ou das regras praticadas na sua caixa de correio electrónico. Além disso, regras conforme indicado no ponto 2.8 sobre documentos e partilha de informação em áreas comuns são igualmente aplicáveis;
- 7.7 é proibido criar, consultar, utilizar caixas de correio electrónico privadas no interior das caixas de correio electrónico atribuídas ao UTILIZADOR DA EMPRESA pela EMPRESA;
- 7.8 A empresa tem de qualquer maneira disponibilizado alguns endereços compartilhados por mais do que um utilizador da empresa, fazendo claro a natureza de não confidencialidade das mensagens. Estes endereços geralmente correspondem a caixas de correio electrónico de Direcções ou de Serviços. De toda a forma, as mensagens externas, enviadas ou recebidas através destas caixas de correio têm que ser guardadas.

## 8. CONTROLO

- 8.1 Em conformidade com o previsto na legislação em vigor, a EMPRESA deve verificar periodicamente os equipamentos informáticos atribuídos aos utilizadores (incluindo telemóveis), a sua utilização e os seus programas e/ou aplicativos relacionados, a fim de detectar eventuais vírus informáticos e garantir a integridade e segurança do sistema, e verificar a sua correcta utilização e assim evitar qualquer acto ou comportamento que possa comprometer a integridade de todos os dados da empresa.
- 8.2 Em conformidade com o previsto na legislação em vigor, a empresa deve efectuar verificações específicas, mas não regulares à utilização das caixas de correio electrónico e internet através da análise de dados agregados, a fim de verificar a correcta utilização dos serviços e de forma a evitar qualquer possível comportamento que poderia comprometer a integridade de todos os dados da empresa.
- 8.3 Se um funcionário tiver autorização para ter acesso a determinadas informações do SISTEMA DE INFORMAÇÃO DA EMPRESA, esta autorização é considerada como estritamente limitada à realização de uma tarefa, de acordo com os formulários de autorização previamente emitidas. A EMPRESA, com o possível apoio da EMPRESA ASSOCIADA, deve efectuar verificações específicas, mas não regulares, de acordo com a legislação em vigor, sobre o perfil dos UTILIZADORES DA EMPRESA, a fim de verificar o acesso e a gestão dos dados da empresa, bem como a consistência entre as tarefas atribuídas, o perfil dado e as autorizações concedidas e descobrir qualquer comportamento que poderia colocar em risco a integridade de todos os dados da empresa.
- 8.4 Os dados analisados durante os controlos não são automaticamente nem sistematicamente associados a UTILIZADORES DA EMPRESA identificados, mas por causa da sua natureza poderiam, através do processamento e a associação dos mesmos com outros dados, identificar os utilizadores da empresa.
- 8.5 No caso de uma violação dos perfis de autorização de acesso aos dados da empresa é determinado que a empresa tem o direito de tomar todas as medidas necessárias para se proteger, considerando estas violações graves incumprimentos legais e do contrato de trabalho.
- 8.6 Os possíveis dados de internet e sua correspondente análise será usada apenas para criar algumas informações estatísticas sobre o uso dos "sites" e também para verificar periodicamente o seu uso correcto e são mantidos apenas por um período de tempo limitado, de acordo com a legislação em vigor.
- 8.7 Todos estes dados podem ser utilizados para a verificação da responsabilidade em caso de possíveis crimes de informações prejudiciais à empresa, bem como em caso de litígio.
- 8.8 Cada funcionário envia notificações de qualquer violação deste CÓDIGO DE CONDUTA TI para o

endereço de correio electrónico [ia-odv@gewiss.com](mailto:ia-odv@gewiss.com), de acordo com o previsto na "Política de Gestão de Irregularidades", disponível no página de intranet e no quadro de avisos da EMPRESA.

- 8.9 A EMPRESA promove o respeito pelas normas de conduta contidas neste documento e deve comunicar imediatamente, também por meio do Responsável de Segurança ou outra pessoa responsável, qualquer violação das normas deste Código ao Responsável de Controlo Interno "Corporate".

## 9. NÃO OBSERVÂNCIA DAS INSTRUÇÕES E SANÇÕES

- 9.1 A não-observância das regras previstas no presente CÓDIGO DE CONDUTA DE TI serão objecto de avaliações disciplinares de acordo com a legislação em vigor, também quanto à sua extensão judicial.
- 9.2 A EMPRESA deverá pedir indemnização às pessoas responsáveis por possíveis danos decorrentes de uma utilização não consciente ou não obediente das regras escritas neste CÓDIGO DE CONDUTA DE TI.
- 9.3 De acordo com a lei, os utilizadores da empresa poderão ser chamados a responder, também sobre o ponto de vista disciplinar, em caso de roubo, perda e possíveis danos ao equipamento informático devido a um uso não consciente do mesmo. O correspondente valor do dano pode ser cobrado através da folha de remunerações.