

Índice

Objeto e Âmbito de aplicação	3
Responsabilidade pelas nossas ações e comportamentos	4
Cumprimento da legislação, das disposições e das regras, normas e instruções internas	4
Respeito dos direitos humanos e condições de trabalho justas	5
Saúde, Segurança, ambiente e integridade do Produto	6
Deveres, Direitos, responsabilidades, e proibições relativas a relações laborais:	6
Direitos da Friemo, SA	6
Deveres da Friemo,SA	7
Direitos dos Trabalhadores	7
Deveres dos trabalhadores	7
Proibições	9
Boa conduta para a prevenção e combate ao assédio no trabalho	11
Proibição da prática de assédio	11
Prevenção da prática de assédio	11
Denúncia da prática de assédio	12
Procedimento	12
Boa conduta e prevenção de corrupção e branqueamento de capitais	13
Cumprimento da legislação antitrust	13
Anticorrupção	14
Branqueamento de Capitais	15
Conflitos de Interesses	15
Utilização do património da Friemo,SA	17
Proteção de dados e cibersegurança	18
Informações confidenciais e propriedade intelectual	18
Normas de importação e exportação	19
Cumprimento das obrigações fiscais	19
Regulamento de utilização das Tecnologias de informação e comunicação	20
Política de «Clean Desk»	20
Documentos	21

Impressora	21
Computador	21
As passwords e o acesso à informação	22
Correio Eletrónico (e-mail)	24
Internet	26
Etiqueta Digital	27
Intranet	28
Partilha de informação ou ficheiros com outros utilizadores	29
Cópias de segurança	30
Controlo de acessos	30
Comunicações internas e externas	31
Segurança e Pagamentos Eletrónicos	31
Dispositivos Móveis	32
Admissão de colaboradores	33
Saída de colaboradores	34

Objeto e Âmbito de aplicação

A Friemo,SA compromete-se a agir com honestidade e integridade. Por conseguinte, tal como descreve a **Visão** e a **Missão** no nossa Política de **Qualidade**, a Friemo,SA tem plena consciência do seu papel na sociedade e da **responsabilidade** a ele associada de contribuir ativamente para um **desenvolvimento sustentável**. Estamos convencidos de que os nossos **princípios e valores** nos permitem crescer de forma sustentável, aportando benefícios para as partes interessadas e para as comunidades em que exercemos a nossa atividade.

Para a Friemo SA, agir de forma sustentável e responsável significa respeitar a lei, preservar os recursos e promover a proteção do clima e do ambiente, assumindo ao mesmo tempo as nossas responsabilidades para com os nossos colaboradores, parceiros, fornecedores e clientes, e para com a sociedade. Estamos firmemente empenhados nos **objetivos de desenvolvimento sustentável das Nações Unidas** (UN Sustainable Development Goals). Por conseguinte, reiteramos o nosso respeito pelos dez **princípios relativos aos direitos humanos, práticas laborais, proteção ambiental e combate anticorrupção** nele contidos.

A Friemo SA reconhece que os desafios jurídicos, sociais e culturais podem variar em função da região geográfica e em tempo. Assim, o presente código de conduta define padrões importantes que, juntamente com os nossos valores corporativos, constituem a base vinculativa das atividades comerciais, laborais e sociais da Friemo SA.

O Código de Conduta prevê que cada colaborador, cada diretor e cada administrador assumam a responsabilidade pelas suas **ações** e comportamento e deve constituir a orientação da empresa para o nosso **comportamento quotidiano**. O presente documento aponta, igualmente, os objetivos **éticos** e **princípios** para a nossa atividade empresarial, laboral e social, e o modo como trabalhamos em conjunto.

O Código de Conduta aplica-se, além disso, a todos os colaboradores, diretores e administradores. O conceito regras neste documento abrange ainda todas as diretivas, manuais, normas e disposições e procedimentos internos a cada nível aprovados ou publicados, de acordo com as disposições do Sistema de Gestão da Qualidade.

A Friemo SA reserva-se no direito de adaptar este Código de Conduta sempre que a situação assim o exigir. Qualquer adaptação será devidamente comunicada. A versão atualmente em vigor é publicada no Sistema de Gestão da Qualidade.

Responsabilidade pelas nossas ações e comportamentos

Na Friemo assumimos pessoalmente a responsabilidade pelas nossas ações e comportamentos e agimos de boa-fé em todas as questões relacionadas com o negócio. No caso de surgirem dúvidas ou sentir qualquer insegurança em relação a instruções recebidas do seu superior hierárquico, pode contactar o seu departamento de gestão de recursos humanos, a fim de verificar se as referidas instruções estão em conformidade com o Código de Conduta ou outras regras, princípios ou instruções da Friemo SA.

Cumprimento da legislação, das disposições e das regras, normas e instruções internas

Na Friemo SA o cumprimento da legislação e disposições aplicáveis é obrigatório. Uma vez que a legislação e disposições em causa podem variar de país para país, não é possível enumerá-las neste Código de Conduta.

Uma violação da legislação e disposições aplicáveis e, por conseguinte, do Código de Conduta, para além de sanções penais, multas e perda de reputação da Friemo SA, pode também ter como consequência sanções pessoais.

Em caso de perguntas ou dúvidas sobre se determinado comportamento é ou não permitido, consulte o seu departamento de relações humanas, ou, tratando-se de diretivas ou políticas internas, contacte a área competente. As regras da Friemo SA abrangem, entre outros, as políticas e manuais sobre (1) Signatários autorizados; (2) Investimentos

financeiros; (3) Conservação de documentos; (4) Regras processuais padronizadas; (5) Integridade do produto; (6) Segurança da informação.

Para facilitar, considere o exemplo abaixo:

Exemplo 1

Você acha que os padrões de segurança não estão provavelmente a ser cumpridos em determinadas instalações da Friemo SA. Que deve fazer?

Comportamento desejável

Contacte o departamento responsável pela aplicação das normas em questão, nomeadamente o responsável pela área da segurança, o departamento de qualidade ou o departamento de relações humanas para que verifiquem a situação.

Respeito dos direitos humanos e condições de trabalho justas

Direitos humanos, condições de trabalho justas e respeito mútuo são, para a Friemo SA, reflexo dos nossos valores corporativos de Elevada Conduta Ética, Trabalho de Equipa, Mérito, compromisso com os Acionistas e Compromisso para com a Sociedade e Ambiente. Estamos convictos de que o empenho no respeito dos direitos humanos e de condições de trabalho justas reforçam o nosso poder de inovação, eficiência e coesão, consolidam as nossas relações com os clientes, fornecedores e outros grupos de interesse e promovem o desenvolvimento económico nos nossos mercados e regiões.

Independentemente do quadro cultural ou jurídico de cada país em que a nossa empresa ou marcas estejam presentes, cada um dos nossos colaboradores deve contribuir para um ambiente de trabalho caracterizado pela confiança e segurança, a todos os níveis hierárquicos. A regra aplica-se, portanto, a todos os colaboradores e a todos os processos da empresa.

Em caso de desconfiança ou preocupação, pode dirigir-se ao seu departamento local de relações humanas.

Saúde, Segurança, ambiente e integridade do Produto

A proteção da saúde e da segurança constituem um elemento fundamental da nossa responsabilidade e atividade empresarial. É nossa obrigação adotar medidas para a proteção da saúde e da segurança, cumprir as disposições e instruções de trabalho e utilizar o equipamento de proteção exigido.

A proteção do ambiente constitui parte integrante da nossa política empresarial. Consideramos que economia e ambiente não têm de se excluir mutuamente. Na Friemo SA ambos constituem a base de uma criação sustentável de valor. Comprometemo-nos a desenvolver e fabricar produtos seguros. Com os nossos processos e produtos, contribuímos de forma considerável para uma gestão sustentável dos recursos, para a proteção do ambiente e para a proteção do clima. Estamos empenhados na preservação dos recursos através da adaptação contínua da nossa produção, da qualidade e desempenho dos nossos produtos em termos do seu impacto ambiental e da redução do consumo de energia, água, matérias-primas e consumíveis.

Estamos todos obrigados, no âmbito das atividades da Friemo, SA a respeitar as normas de trabalho e proteção do ambiente. Caso tenha dúvidas ou observações a apresentar relacionadas com estas questões no seu local de trabalho, contacte o seu superior hierárquico, o Técnico superior de Segurança e Saúde no Trabalho, o Técnico superior de Ambiente ou o seu departamento de gestão de recursos humanos.

Deveres, Direitos, responsabilidades, e proibições relativas a relações laborais:

Para garantir um entendimento de todas as partes em matéria laboral, a Friemo SA define as seguintes orientações relativas a direitos, deveres e proibições das partes envolvidas:

Direitos da Friemo SA

1. Beneficiar dos resultados de trabalho exercido pelos seus funcionários conforme prevê o contrato de trabalho;
2. Definir as atividades e tarefas dos funcionários, salvaguardando as normas jurídicas e o contrato de trabalho;

3. Definir ordens de serviço e diretivas relativas ao trabalho, salvaguardando as normas jurídicas e o contrato de trabalho.

Deveres da Friemo SA

1. Respeitar e tratar com urbanidade e probidade o trabalhador;
2. Proporcionar boas condições de trabalho, quer do ponto de vista físico quer moral;
3. Pagar pontualmente a retribuição adequada ao trabalho;
4. Contribuir para a elevação do nível de produtividade do trabalhador;
5. Respeitar a autonomia técnica do trabalhador cuja regulamentação profissional o exija;
6. Possibilitar o exercício de cargos em organizações representativas dos trabalhadores;
7. Prevenir riscos e doenças profissionais, salvaguardando as informações e formações necessárias acerca da proteção da segurança e saúde do trabalhador no que respeita à prevenção de riscos de acidentes e doenças;
8. Manter atualizado o registo dos trabalhadores (todos os seus dados pessoais e profissionais).

Direitos dos Trabalhadores

1. Receber da empresa a remuneração mensal correspondente à prestação do seu trabalho;
2. Ter a sua prestação e conduta salvaguardada ao abrigo dos regulamentos e políticas de gestão de pessoas na Friemo SA e, em tudo o que por esta via não seja previsto, pela aplicação do instrumento de regulamentação coletiva aplicável ou pela lei vigente.

Deveres dos trabalhadores

1. Tratar com urbanidade as instalações da Friemo,SA, zelando pelos interesses comuns da empresa e demais colaboradores;

2. Utilizar de forma responsável e ética qualquer recurso natural durante a permanência nas instalações da Friemo SA, respeitando a política de Ambiente e Segurança em matéria de Desenvolvimento Sustentável e Responsabilidade Social, bem como todos os regulamentos de normas e condutas a adotar internamente;
3. Conhecer as regras de separação de resíduos, comprometendo-se a separar quaisquer resíduos inorgânicos durante a estadia nas instalações da empresa, utilizando os devidos depósitos para o efeito;
4. Em caso de perda, extravio ou danificação por utilização negligente de qualquer equipamento que me foi entregue, suportar o custo de aquisição de novo equipamento;
5. Entregar os equipamentos que me forem cedidos pela Friemo SA em caso de término da relação laboral;
6. Ter conhecimento que qualquer objeto pessoal deve ser guardado nos cacifos;
7. Ter conhecimento que a Friemo não se responsabiliza por qualquer objeto pessoal de qualquer colaborador;
8. Respeitar e tratar com urbanidade e lealdade a entidade, os superiores hierárquicos, os companheiros de trabalho e as demais pessoas que estejam ou entrem em relações com a empresa;
9. Comparecer com assiduidade e pontualidade no posto de trabalho e realizar o trabalho com zelo e diligência;
10. Utilizar com cuidado, e zelar pela boa conservação dos equipamentos e demais bens que lhe sejam confiados;
11. Guardar lealdade à organização, nomeadamente não negociando por conta própria ou alheia em concorrência com ela, nem divulgando informações referentes à sua organização, métodos de produção ou negócios;
12. Cumprir as ordens e instruções dos superiores hierárquicos em tudo o que respeite a execução e disciplina do trabalho, bem como segurança e saúde no trabalho e cooperar para a melhoria desta;

13. Cumprir as prescrições sobre segurança e saúde no trabalho que decorram da lei ou do CCT;
14. Cumprir o regulamento interno da empresa, tal como quaisquer ordens e instruções de serviço;
15. Contribuir para a melhoria da produtividade da empresa;
16. Participar de modo diligente em ações de formação profissional que lhe sejam proporcionadas pelo empregador;
17. Participar no sistema de avaliação de desempenho;
18. Apresentar-se ao trabalho com a sua capacidade profissional intacta, sendo proibido executar o trabalho sob o efeito de álcool ou estupefacientes.

Proibições

No âmbito de uma coabitação urbana, cívica, e de salvaguarda dos interesses de todos as partes interessadas, são estipuladas as seguintes proibições para colaboradores com vínculo laboral, em regime de prestação de serviços ou prestação de trabalho temporário:

1. Ocupar-se de qualquer atividade que possa prejudicar os interesses da empresa, bem como a utilização de máquinas, computadores, telefones, entre outros, disponíveis no ambiente de trabalho, para uso pessoal, sem autorização superior.
2. Retirar do local de trabalho, sem prévia autorização, qualquer equipamento, objeto ou documento;
3. Participar em empresas ou iniciativas que concorram diretamente com quaisquer atividades da Friemo SA ou do grupo em que se insere.
4. Divulgar, por qualquer meio, assunto ou facto de natureza privada da Empresa;
5. Fumar no ambiente interno e/ou fora das pausas estipuladas e em locais proibidos;
6. Promover algazarra, brincadeiras e discussões durante o tempo de trabalho;
7. Recorrer a vocabulário ou gestos impróprios à moralidade e respeito, nas dependências da empresa;

8. Propagar ou incitar a insubordinação ao trabalho;
9. Aplica-se também neste Regulamento todas as restantes proibições inerentes a cada posto de trabalho, área ou departamento e que tenham sido comunicadas formalmente.

Boa conduta para a prevenção e combate ao assédio no trabalho

Proibição da prática de assédio

Entende-se por assédio o comportamento indesejado, nomeadamente o baseado em fator de discriminação, praticado aquando do acesso ao emprego ou no próprio emprego, trabalho ou formação profissional, com o objetivo ou o efeito de perturbar ou constranger a pessoa, afetar a sua dignidade, ou de lhe criar um ambiente intimidativo, hostil, degradante, humilhante ou desestabilizador. É proibida a prática de qualquer ato de assédio no local de trabalho ou fora do local de trabalho, se em circunstâncias relacionadas com este.

Constitui assédio sexual o comportamento indesejado de carácter sexual, sob forma verbal, não verbal ou física, com o objetivo ou o efeito referido no número anterior.

Constitui assédio moral um conjunto de comportamentos indesejados, percecionados como abusivos, praticados de forma persistente e reiterada, podendo consistir num ataque verbal com conteúdo ofensivo ou humilhante ou em atos subtis, que podem incluir violência psicológica ou física.

Prevenção da prática de assédio

Constituem medidas preventivas da prática de assédio, designadamente as seguintes:

a) Fomentar uma cultura organizacional de cooperação e respeito entre os trabalhadores e outros intervenientes no ambiente de trabalho e normal funcionamento da Friemo SA.

b) Garantir a existência de um canal de comunicação eletrónico interno que garanta o sigilo e a integridade das denúncias efetuadas, nomeadamente <https://denuncias.friemo.pt>;

c) Instaurar procedimento disciplinar na sequência do conhecimento de denúncias de factos que indiciem a prática de assédio;

d) Salvaguardar a confidencialidade no tratamento de toda a informação referente às vítimas e/ou denunciantes e/ou testemunhas, bem como ao conteúdo das participações, na estrita observância do quadro legal instituído;

e) Assegurar a inexistência de quaisquer represálias subsequentes sobre os denunciadores da prática de assédio, sempre que as mesmas se verificarem verdadeiras ou não seja provada má-fé na denúncia;

Denúncia da prática de assédio

Todos aqueles, a quem o presente Código se aplica, que sejam alvo, testemunhem ou que tenham conhecimento de factos suscetíveis de constituir a prática de assédio, devem denunciá-los, bem como colaborar nos procedimentos a realizar conseqüentemente.

As denúncias devem ser registadas e conter uma descrição circunstanciada dos factos suscetíveis de constituir a prática de assédio, com indicação do dia, da hora e do local em que ocorreram, e com identificação da vítima ou vítimas, do assediante ou assediadas e de eventuais meios de prova, testemunhal ou outra, bem como do denunciante, caso não seja a própria vítima.

As denúncias devem ser reportadas à direção de Gestão de Recursos Humanos da Friemo SA através do formulário “relatório de incidente”, disponível no mesmo departamento.

Procedimento

Recebida a denúncia, o departamento de Gestão de Recursos Humanos da Friemo SA e a administração são responsáveis por investigar a veracidade da prática de assédio e, conseqüentemente, por instaurar o procedimento disciplinar ao denunciado, caso conclua existirem indícios suficientes para tal.

O procedimento disciplinar a instaurar ao denunciado não prejudica a sua responsabilidade civil, contraordenacional, e, eventualmente, criminal.

Caso se comprove que o denunciante e testemunhas agiram com dolo, no intuito de prejudicar outro, apresentando denúncia infundada, contendo matéria difamatória ou injuriosa, serão os mesmos sancionados disciplinarmente.

Boa conduta e prevenção de corrupção e branqueamento de capitais

Cumprimento da legislação antitrust

A legislação Antitrust pretende proteger a livre concorrência e garantir a defesa dos interesses dos nossos clientes e demais consumidores. Na Friemo SA cumprimos qualquer legislação antitrust aplicável, nomeadamente leis e disposições em matéria de monopólios, concorrência desleal, restrições comerciais e da concorrência e sobre as relações com a concorrência e com os clientes.

Temos plena consciência de que a violação das regras da concorrência pode levar à anulação de contratos, a sanções penais e pecuniárias, e à perda de reputação da empresa e das suas marcas. Sempre que surgirem dúvidas quanto ao facto de determinada situação estar ou não em conformidade com a legislação antitrust, consulte imediatamente o departamento de gestão de Recursos Humanos ou denuncie a situação através do canal interno de denúncias através do sítio online <https://denuncias.friemo.pt>.

O exemplo 2 ajuda a compreender situações de dia-a-dia, em que qualquer um de nós pode incorrer na violação de leis Antitrust.

Exemplo 2

Num evento local encontra um antigo colega por acaso, que agora trabalha para a concorrência. Ambos recordam tempos antigos, quando o seu ex-colega lhe pergunta se na Friemo SA ainda produzem o mesmo tipo de mesas por medida a pedido do cliente, e, ainda se já aumentaram os preços de determinado produto, devido ao aumento dos preços das matérias-primas. Como é que reage?

Comportamento desejável

Deve esclarecer que não tem autorização para falar desses assuntos com pessoas externas à organização. Sejam quais forem as circunstâncias, não pode nunca fornecer informações/respostas a perguntas que impliquem o intercâmbio de informações sensíveis do ponto de vista económico ou de processo. Caso a questão

surja de concorrentes comunique o facto ao diretor de fábrica ou ao departamento de gestão de recursos humanos.

Anticorrupção

Corrupção é a utilização abusiva do poder ou da confiança conferidos a uma pessoa por entidades públicas ou privadas com base no compromisso por parte dessa pessoa de não obter, no âmbito do exercício desses poderes e autoridade, quaisquer vantagens indevidas para si própria.

As nossas relações comerciais, laborais e comunitárias pautam-se pela integridade, e cumprimos rigorosamente todas as leis e disposições anticorrupção, incluindo nomeadamente as que se referem ao suborno de colaboradores estrangeiros, recrutamento favorecido, aliciamento de parceiros entre outros. Esforçamo-nos por construir relações positivas e de cooperação com os nossos clientes, fornecedores, colaboradores e stakeholders.

A oferta e aceitação de incentivos, presentes e favores fazem muitas vezes parte do dia a dia no mundo dos negócios. Na maior parte dos casos, trata-se de convites para almoços, jantares e eventos. Estes convites e pequenos presentes podem reforçar as relações, mas não os utilizamos para influenciar de forma desleal relações comerciais ou decisões. Assim, limitamos a aceitação de presentes e a oferta de presentes a 50€, recusamos e não toleramos qualquer forma de corrupção, suborno, roubo, fraude, extorsão ou pagamento ilícito. Não fazemos pagamentos ilícitos a nenhuma pessoa singular, empresa, organização internacional ou entidade pública nem lhes concedemos quaisquer outras vantagens ilegais com o objetivo de influenciar processos de decisão, violando as leis em vigor.

Não oferecemos, concedemos, exigimos ou recebemos quaisquer subornos, pagamentos ilegais, luvas, comissões, incentivos, presentes generosos, almoços, jantares, convites para eventos, favores ou quaisquer outros benefícios ou donativos de valor pela concretização de oportunidades de negócio com a Friemo SA ou relacionadas com a sua atividade empresarial.

A violação das leis anticorrupção pode levar à anulação de contratos e a sanções penais e pecuniárias. Qualquer envolvimento em atos de corrupção prejudica a Friemo SA

Exemplo 3

A Friemo, SA está a planear uma nova fábrica no município de V.N.Gaia, para aumentar a sua capacidade. Para a construção do edifício são necessárias diversas autorizações e concessões do município. Depois de esperar vários meses pela respetiva documentação, começa a pensar que, provavelmente, um incentivo ao membro do município com influência na decisão em questão que está a tratar do seu pedido poderá acelerar o processo de aprovação, e que tal será benéfico para todos, incluindo os cidadãos locais, para quem serão criadas novas oportunidades de trabalho.

Comportamento desejável

Mesmo que saiba que tem direito à concessão das autorizações, e que será benéfico para todas as partes, uma tentativa deste tipo para influenciar o processo de aprovação é classificada como corrupção pela legislação de qualquer país membro da UE. Além disso, ela constitui uma violação clara das diretivas de combate à corrupção da Friemo SA. Deve pôr tal ideia completamente de parte e familiarizar-se com a diretiva de combate à corrupção da Friemo SA

Branqueamento de Capitais

O branqueamento de capitais consiste na transformação de lucros resultantes de atividades criminosas, por exemplo, evasão fiscal, em valores patrimoniais aparentemente legítimos. Em termos de branqueamento de capitais, considera-se que existe um risco elevado quando os pagamentos são efetuados por terceiros e não pelo próprio cliente.

Conflitos de Interesses

A Friemo,SA respeita o direito dos seus colaboradores se dedicarem a atividades extraprofissionais de natureza privada que de nenhum modo possam entrar em conflito com as atividades ou ter um reflexo negativo na Friemo,SA ou na imagem da empresa. Assim, não é permitido cultivar direta ou indiretamente relações e interesses comerciais ou

financeiros que se oponham aos interesses da Friemo,SA ou prejudiquem a sua eficiência no cumprimento pleno das suas obrigações no quadro da sua relação laboral, defendendo os superiores interesses da Friemo,SA. Pode haver conflito de interesses nos seguintes casos:

- Se, no caso de trabalhadores, para além do trabalho prestado na Friemo,SA, existir uma relação laboral com outra empresa, sobretudo se essa outra empresa for um concorrente, cliente ou fornecedor da Friemo,SA (ou se se tratar de uma empresa com probabilidade de vir a ser em breve concorrente, cliente ou fornecedor);
- Se, no caso de trabalhadores, existir relações comerciais com uma sociedade da qual um familiar é acionista, intervém na administração ou de qualquer outro modo detém uma participação relevante na sociedade;
- Se, no âmbito do exercício das funções na Friemo,SA, negociar ou especular com materiais, equipamentos ou consumíveis que são comprados pela Friemo,SA, ou negociar por conta própria com produtos vendidos pela Friemo,SA, ou que sejam propriedade da Friemo,SA;
- Se, no caso de responsável por gestão de pessoas, influenciar decisões a favor de familiares ou outros da esfera pessoal, como decisões de recrutamento, revisão salarial, promoção ou outras, não devendo haver lugar a liderar pessoas com quem se mantenha uma relação familiar; ainda neste âmbito, sempre que se proporcionarem relações pessoais que possam ser suscetíveis de interferir com o normal funcionamento dos procedimentos da Friemo,SA, por exemplo, por envolverem conhecimento de matérias confidenciais afetas às pessoas com quem se mantém relação ou a outras que lhe são próprias, tal deve ser comunicado ao departamento de Gestão de Recursos Humanos a fim de ser elaborado um plano de prevenção de conflitos de interesses.

Exemplo 3

A Friemo,SA está a consultar o mercado para encontrar um fornecedor de novos materiais para fazer face ao aumento de pedidos que tem tido.

Comportamento desejável

Em determinadas circunstâncias, a celebração de um contrato com a empresa do seu irmão pode ser aceitável, e do interesse da Friemo, SA. Comunique a relação de parentesco ao seu superior hierárquico e ao departamento de compras e assegure-se de que não intervém no processo de concurso nem nas decisões com ele relacionadas. Em caso de dúvida dirija-se ao departamento gestão de recursos humanos.

Utilização do património da Friemo,SA.

Todos os envolvidos com o negócio da Friemo,SA, entre colaboradores, fornecedores, clientes, ou outros, devem respeitar o tratamento urbano entre si, bem como relativamente à propriedade da Friemo,SA. O Património empresarial da Friemo, SA inclui bens físicos, como produtos fabricados, equipamentos de produção ou administrativos., ferramentas, instalações, veículos entre outros, bem como bens imateriais, como sejam o seu conhecimento e direitos de propriedade intelectual.

Assim, é da responsabilidade de todos a adoção das seguintes orientações de conduta:

- (1) com urbanidade as instalações da Friemo, SA, zelando pelos interesses comuns da empresa e demais colaboradores.
- (2) utilizar de forma responsável e ética qualquer recurso natural durante a permanência nas instalações da Friemo, SA, respeitando a política de Ambiente e Segurança em matéria de Desenvolvimento Sustentável e Responsabilidade Social;
- (3) conhecer as regras de separação de resíduos, comprometendo-se a separar quaisquer resíduos inorgânicos durante a estadia nas instalações da empresa, utilizando os devidos depósitos para o efeito;
- (4) ter conhecimento que só é permitido fumar em espaços restritos e devidamente identificados;

(5) ter conhecimento que, em caso de perda, extravio ou danificação por utilização negligente de qualquer equipamento, o custo de aquisição de novo equipamento será suportado pelo autor da infração;

(8) Ter conhecimento que a Friemo, SA não se responsabiliza por qualquer objeto pessoal, seja de colaborador, visitante ou outro, que seja danificado, extraviado ou perdido nas suas instalações.

Proteção de dados e cibersegurança

Na Friemo, SA existe uma política de utilização responsável de equipamentos e tecnologias de informação a ser cumprida, que salvaguarda o utilizador bem como os dados de negócio e pessoais a serem usados no âmbito da atividade da Friemo, SA. O cumprimento desta política determina a segurança e proteção divulgação de informações confidenciais e segredos comerciais ou o roubo ou utilização abusiva de dados pessoais pertencentes a qualquer dos intervenientes no negócio da Friemo, SA.

Informações confidenciais e propriedade intelectual

A proteção de informações comerciais confidenciais e segredos comerciais («informações confidenciais») é imprescindível para salvaguarda dos interesses e do sucesso da Friemo, SA. Assim, cada colaborador é responsável por garantir que as informações confidenciais a que tem acesso no âmbito da sua atividade laboral são rigorosamente tratadas de forma confidencial, não sendo utilizadas de forma abusiva nem divulgadas junto de colegas ou de terceiros.

A utilização abusiva ou divulgação de informações confidenciais, poderá ser alvo de medidas disciplinares e até despedimento, mesmo que não se verifique um benefício pessoal da divulgação em causa. Tal pressuposto mantém-se mesmo após término da relação contratual, garantindo que o património desta natureza, incluindo as informações confidenciais, são imediatamente devolvidos à Friemo, SA, podendo o contrário ser alvo de processo civil.

Normas de importação e exportação

A Friemo, SA. Cumpre todas as normas em matéria de importação e exportação nomeadamente no que diz respeito a sanções, embargos e demais leis, disposições, decretos ou diretivas governamentais, bem como todas as regulamentações de transporte ou envio de bens e tecnologia determinadas pelo grupo.

Cumprimento das obrigações fiscais

A Friemo,SA está certa das suas obrigações fiscais, e declara-se explicitamente a favor da observância das disposições nacionais e internacionais em matéria de legislação tributária.

Regulamento de utilização das Tecnologias de informação e comunicação

Atualmente, dada a constante inovação da tecnologia informática, é cada vez mais frequente a criação, por parte das organizações, de políticas, processos e guias para o utilizador da informação, a fim de garantir a segurança dos dados confidenciais de negócios e dos dados pessoais tratados, sobretudo online e em formato digital. Deste modo, seguem-se breves regras e procedimentos a adotar por todos os colaboradores.

Política de «Clean Desk»

A política de «clean desk» visa essencialmente que o posto de trabalho de cada um dos colaboradores esteja limpo e organizado. Assim, deverão os colaboradores observar boas práticas para a implementação de uma política de «clean desk», como as seguintes:

- a) O posto de trabalho de cada colaborador deve estar sempre arrumado e organizado;
- b) Toda a documentação confidencial deve ser mantida num local com acesso restrito. Cabe a cada colaborador que, no exercício das suas funções, trate documentação confidencial informar o seu superior hierárquico da necessidade de a arquivar em local de acesso restrito de forma a serem providenciados os meios para esse efeito;
- c) Nenhuma Informação Confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrónicos ou não;
- d) Após reuniões ou visitas, internas ou externas, todo o material utilizado deverá ser retirado das salas de reuniões, incluindo as anotações realizadas;
- e) Deve evitar-se a ligação equipamentos elétricos tais como ventoinhas, aquecedores, etc. no mesmo circuito eletrónico;
- f) Durante as reuniões, com temas confidenciais ou sensíveis, os colaboradores devem verificar se a sala está corretamente fechada e protegida para que a informação seja partilhada de forma totalmente confidencial;

No fim do dia de trabalho os colaboradores devem verificar se as portas e janelas ficam corretamente fechadas.

Documentos

- a) Os documentos, impressões, agendas e blocos de apontamentos com dados confidenciais devem ser tratados de forma a garantir que terceiros não possam ter conhecimento do seu conteúdo;
- b) Documentos com dados médicos e dados de menores são muito sensíveis pelo que o cuidado na sua utilização e tratamento deve ser redobrado;
- c) Os colaboradores devem evitar recolher, tratar e reunir dados pessoais em papel ou em formato eletrónico sem acautelar a autorização explícita e informada do Titular dos Dados, devendo informar de cada recolha e tratamento efetuado;
- d) Sempre que o colaborador se afaste do seu posto de trabalho deve colocar os documentos dentro de armários ou gavetas devidamente trancadas devendo, quando necessário, solicitar ao superior hierárquico os meios necessários para esse efeito;
- e) As impressões devem ser recolhidas da impressora o mais rapidamente possível.

Impressora

- a) As impressoras deverão ser utilizadas para atividades relacionadas com o negócio e atividade apenas;
- b) Tratando-se de documentos confidenciais e/ou áreas funcionais que impliquem o manuseamento de documentos altamente confidenciais, que contenham informações ou dados pessoais sensíveis, o colaborador deverá predefinir o procedimento de impressão segura;
- c) Na impressão de documentos confidenciais o colaborador deve acompanhar presencialmente a saídas das folhas ou, em alternativa, utilizar o procedimento de impressão segura, garantindo em ambos os casos que todas as folhas são recolhidas da impressora;

Computador

- a) Quando o colaborador não esteja a utilizar o seu computador deve bloquear a sessão (Ctrl + Alt + Del);

- b)** O ambiente de trabalho deverá estar limpo e organizado («clean screen»);
- c)** O ambiente de trabalho não deve conter ficheiros que contenham informação sensível e confidencial, desta forma garantindo que a mesma não seja acedida ou removida com facilidade;
- d)** O computador apenas tem software autorizado e devidamente licenciado. Deve evitar-se o armazenamento de dados em pastas locais, todos os documentos de trabalho devem estar armazenados na onedrive, sharepoint ou no servidor de ficheiros;
- e)** Não é permitido o download, instalação ou transferência, sob qualquer forma, de aplicações, programas, ferramentas ou mecanismos nos computadores disponibilizados, sem a prévia autorização da área de IT.

As passwords e o acesso à informação

As *passwords* (palavras-chave) são pessoais e intransmissíveis. Deste modo, destacamos algumas regras relativas às passwords e ao acesso à informação que os colaboradores deverão adotar ao longo do desenvolvimento da sua prestação de trabalho. São elas:

- a)** Manter as passwords confidenciais;
- b)** Utilizar passwords com um mínimo de 8 caracteres;
- c)** Utilizar, na construção da password, pelo menos três das seguintes premissas: letra maiúscula, letra minúscula, número ou carácter especial;
- d)** Alterar as passwords de 180 em 180 dias;
- e)** Não introduzir espaços na sua composição;
- f)** Não reutilizar passwords antes de cinco alterações;
- g)** Não utilizar informação de índole pessoal, como por exemplo, nomes próprios, apelidos, número de telefone, número de cartão de cidadão ou outro documento de identificação, datas de nascimento, matrículas de automóvel, etc.;
- h)** As passwords fornecidas por defeito deverão ser imediatamente alteradas pelos colaboradores;

- i) A geração das passwords deve ser aleatória;
- j) As passwords não deverão ser escritas em locais visíveis e facilmente acessíveis;
- k) As passwords deverão ser alteradas imediatamente, sempre que se suspeite da sua revelação;
- l) Guardar as passwords em softwares encriptados (ex. KeePass);
- m) Não gravar as passwords de forma automática nos sistemas;
- n) Não utilizar as mesmas passwords para os sistemas da organização e sistemas pessoais;
- o) Utilizar passwords seguras, mas fáceis de memorizar;
- p) Implementar e respeitar o mecanismo de atribuição e reativação de passwords que permita a correta identificação do utilizador que a solicita ou recebe;
- q) O sistema de alteração de palavras-chave deverá adotar, preferencialmente, um procedimento de confirmação de modo a permitir a identificação de erros de introdução (ex. exigir que a mesma palavra-passe seja inserida duas vezes antes de a aceitar);
- r) As palavras-chave não deverão ser apresentadas no monitor quando estiverem a ser inseridas;
- s) As palavras-chave são informações confidenciais, pelo que sempre que estejam armazenadas em suporte magnético ou quando transmitidas através da rede, deverão estar encriptadas;
- t) Sempre que um sistema aplicacional providenciar a sua própria segurança através de palavra-chave própria, deverão ser utilizadas palavras-chave diferentes nos vários níveis de segurança;
- u) Não deverão ser utilizados mecanismos de login automáticos, isto é, onde não seja solicitada a introdução de uma palavra-chave;
- v) No momento de saída de um colaborador o acesso e password caducam ficando inacessíveis.

**AS PASSWORDS MAIS
UTILIZADAS SÃO:**

COMO CRIAR PASSWORDS SEGURAS:

1. ^a «123456» 2. ^a «password» 3. ^a «qwerty» 4. ^a «abcd1234» 5. ^a data de nascimento	Construir uma frase e utilizar as iniciais de cada palavra.
--------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------

Correio Eletrónico (e-mail)

O correio eletrónico (e-mail) é uma ferramenta de trabalho e deve ser utilizada de forma profissional e cuidada. A utilização imprudente ou inadequada pode dar origem a ataques aos sistemas e à informação existente.

Assim, na utilização do e-mail, deverão ser adotadas as seguintes boas práticas:

- a) O serviço de correio eletrónico (e-mail) deverá ser apenas utilizado para os fins estritamente relacionados com as funções e tarefas que cada colaborador tem atribuídas na organização, sem se permitir o uso para fins particulares/pessoais;
- b) Os utilizadores são responsáveis por todas as atividades realizadas nas suas contas de correio e respetivas caixas de correio, e não deverão permitir a utilização das suas credenciais por pessoas não autorizadas;
- c) Qualquer ficheiro introduzido na rede corporativa ou no posto de trabalho do utilizador através de mensagens de e-mail provenientes de redes externas deve cumprir os requisitos estabelecidos nesta política e, em especial, as que se referem a propriedade intelectual e a controlo de vírus;
- d) Se houver entradas ou saídas de dados através de sistemas de transferência de ficheiros, através de redes públicas não protegidas, é necessário a sua proteção através da criptografia prévia, para que somente possam ser lidos pelo seu destinatário;
- e) Não é permitido participar em atividades de disseminação de correntes de cartas, esquemas em pirâmide ou similares;
- f) Não é permitido difundir conteúdos ilegais, religiosos ou políticos;
- g) É proibido efetuar ataques para obstruir sistemas informáticos dirigidos a um utilizador ou ao próprio sistema de correio, ou qualquer atividade que tenha como objetivo a paralisação do serviço por saturação de linhas de comunicação, da

capacidade de processamento do servidor, ou qualquer atividade com um objetivo semelhante;

- h)** Utilizar o email de forma segura, produtiva, profissional e educada;
- i)** Não reenviar emails com brincadeiras nem reagir por impulso ao conteúdo;
- j)** Verificar sempre os endereços dos destinatários;
- k)** Não abrir emails e ficheiros de origem desconhecida;
- l)** Nunca enviar informação pessoal que seja solicitada por email (v.g. número do cartão de crédito; username; password; nomes; etc.);
- m)** Não seguir as ligações (links) de emails suspeitos;
- n)** Escrever o endereço diretamente no browser;
- o)** Informações críticas de negócio ou dados pessoais só podem ser enviados em formato encriptado. As passwords devem ser enviadas por outro meio de comunicação;
- p)** Caso o e-mail a enviar contenha informação extremamente confidencial deverá ser incluído no assunto a expressão «*confidencial*» e o mesmo deve ser remetido como confidencial para o destinatário, mediante definição prévia na caixa de e-mail utilizada através dos seguintes passos: *mensagem > opções de mensagem > propriedades > definições > confidencialidade > confidencial*;
- q)** Nos departamentos que tratem ou enviem regularmente informação extremamente confidencial deverá ser incluída uma nota de rodapé de um termo de confidencialidade, nos seguintes termos:

«Esta mensagem e documentos eventualmente em anexo destinam-se exclusivamente às pessoas nela indicadas como destinatários e contém matéria confidencial. Se receber esta mensagem por engano, agradecemos contacto por email ou por telefone e eliminação da mensagem e anexos, sem reprodução ou transmissão a quaisquer terceiros / *This message and any files attached hereto is intended only for the addresses mentioned hereinabove and contains confidential information. If you have received this message in error, please notify us by e-mail or by telephone and delete this message and any files attached, without reproduction or communication to any third parties*».

Internet

Vivemos no mundo da informação e a comunicação é a chave do sucesso pessoal e empresarial. Por este motivo é fundamental garantir que a comunicação é realizada de forma adequada, através dos meios pertinentes, e que é transmitida apenas a informação necessária. Para esse efeito os colaboradores devem seguir as regras elencadas abaixo com o objetivo único de melhorar a segurança da informação:

- a) O acesso à Internet só deverá ser realizado para atividades relacionadas com o negócio e exercício da atividade das empresas que constituem o grupo. Não é permitido aos colaboradores acederem a servidores Web não apropriados, como por exemplo:
 - i. Servidores *Web* que contêm imagens sexualmente explícitas ou afins;
 - ii. Servidores *Web* que advoguem atividades e conteúdos ilícitos e inadequados;
 - iii. Servidores *Web* que advoguem a intolerância, racismo, discriminação, xenofobia, violência ou outros desvalores sociais;
- b) Não é permitido utilizar serviços públicos de e-mail, de transferência de ficheiros e ou serviços *cloud* para partilha de dados da organização;
- c) Não é permitido divulgar informação confidencial do negócio nas redes sociais, sem prévia autorização expressa da Administração;
- d) Os colaboradores deverão assegurar que os elementos, dados, comunicações ou materiais que disponibilizam na Internet não têm conteúdo impróprio, ofensivo ou desrespeitoso ou que, de alguma forma, comprometem a imagem da empresa;
- e) Não é permitido utilizar ferramentas da internet para criar ou traduzir conteúdos sensíveis ou confidenciais;
- f) Não é permitido jogar ou fazer apostas online com os recursos da organização (Internet, Computadores, etc.);
- g) Os colaboradores deverão certificar-se que o *site* utilizado é seguro através de duplo clique sobre o cadeado no canto superior esquerdo do ecrã ou que o acesso é feito pelo endereço (*URL*) começado por «*https://*» e não por «*http://*»;

- h) Os colaboradores devem certificar-se que o browser e o antivírus estão atualizados e que utilizam um firewall seguro;
- i) Evitar clicar em hiperligações (*links*) ou fazer *downloads* de fontes desconhecidas;
- j) Todos os programas de proveniência duvidosa não deverão ser executados. Adicionalmente, deverá estar desativada a opção de execução automática de *javascripts* nos *browsers*;
- k) Sempre que se fizer upload de material para a Internet, deverá ser assegurado que os acordos de licenciamento e/ou de *copyright* desse material estão a ser cumpridos;
- l) Sempre que se fizer *download* de material da Internet, deverá ser assegurada a propriedade intelectual e/ou o *copyright* do seu proprietário. Além disso, deverão ser acauteladas as regras de segurança associadas a receção de informação vinda do exterior que possam conter vírus ou código malicioso;
- m) É proibido o acesso a serviços ou fóruns de chat ou sites de redes sociais não permitidos pela empresa;
- n) Procurar previamente informações sobre o cliente, fornecedor ou parceiro.

Etiqueta Digital

Existem também boas práticas a observar por todos os colaboradores no que respeita à comunicação e comportamento na Internet. A “Etiqueta Digital” é constituída por um conjunto de regras sociais – formais ou informais, convencionadas ou naturais, que regulam o comportamento e a comunicação dos utilizadores da internet, promovendo a qualidade da socialização e a eficácia comunicativa.

Desta forma, os colaboradores, no uso da internet, deverão observar o seguinte:

- a) Evitar escrever mensagens em maiúsculas, com cores e a bold;
- b) Ser claro e objetivo, produzir textos simples e com cuidado gramatical e ortográfico;
- c) Ser educado e simpático, agradecer e cumprimentar;
- d) Livre uso de smiles nas comunicações internas, é uma forma simples de facilitar a compreensão daquilo que é escrito;

- e) Não reagir de forma emotiva evitando e-mails ou partilhas desnecessárias;
- f) Antes de publicar alguma informação verificar se o conteúdo:
 - i. Tem interesse;
 - ii. Tem qualidade, é atual e respeita a missão da organização;
 - iii. Tem o formato correto e está a ser publicado no dia, hora e local correto.

Intranet

Na Friemo,SA dispomos de uma rede virtual empresarial privada com acessos controlados e restritos que permitem a criação, armazenamento, partilha e consulta regular de informação inerente ao exercício da atividade da empresa. A rede privada virtual apresenta-se, deste modo, como uma verdadeira base de dados, incluindo todos os documentos e informações das várias empresas que constituem o grupo, pelo que os colaboradores deverão ter em conta as regras abaixo enunciadas:

- a) O acesso à rede é atribuído com a admissão do colaborador, sendo eliminado imediatamente com a cessação do respetivo vínculo contratual, ou imediatamente em situações que o justifiquem de acordo com os procedimentos e políticas internas relevantes nesta matéria;
- b) O acesso a determinadas pastas da rede privada é determinado pelo superior hierárquico em coordenação com o *owner* da pasta em causa, mediante pedido do colaborador a ambos, com a indicação do motivo justificativo do acesso; Caso o acesso seja concedido, o superior hierárquico comunica à área de IT, sendo a mesma responsável pela operacionalização da concessão do acesso;
- c) Os colaboradores deverão aceder e consultar as pastas partilhadas de forma responsável, garantindo a integridade da informação existente e a sua organização; os colaboradores deverão abster-se de eliminar, mover ou alterar pastas partilhadas de acesso conjunto sem autorização para o efeito;

- d)** A criação de pastas e a disposição da informação em cada uma delas deve ser realizada de forma metódica, organizada, restrita e deve cingir-se a informação atualizada, correta e estritamente necessária;
- e)** O acesso à rede fora do local de trabalho deverá ser feito com cautela, de forma a assegurar que a informação acedida não é disponibilizada ou está ao alcance de terceiros;
- f)** Não é permitido a um colaborador assumir indevidamente a identidade de outro nem autorizar que assumam a sua;
- g)** Não é permitido aos colaboradores adicionar *bridges*, *routers*, *gateways*, ou *modems* ou outros à sua estação de trabalho.

Partilha de informação ou ficheiros com outros utilizadores

- a)** A partilha de informação, seja entre colegas de trabalho seja para terceiros, entidades externas, clientes, fornecedores ou parceiros, deverá ser feita na medida do estritamente necessário;
- b)** O colaborador que partilhe informação nos termos da alínea anterior, deverá assegurar-se que os seus destinatários estão obrigados à salvaguarda e confidencialidade dessa informação, mediante acordo de confidencialidade, cláusulas ou obrigações resultantes de contrato ou no âmbito das normas deontológicas da profissão exercida;
- c)** Os colaboradores devem observar um especial cuidado com os dados pessoais que trocam com os parceiros externos e em especial com parceiros fora da UE;
- d)** A disponibilização de informação que contenha dados pessoais deverá respeitar todas as normas e procedimentos internos em matéria de proteção de dados;
- e)** Os colaboradores devem observar especial cuidado ao enviar dados pessoais, sendo que os mesmos deverão preferencialmente estar encriptados ou protegidos;
- f)** A informação disponibilizada deverá ser oficial, correta e autorizada, devendo respeitar as regras;

- g) Sempre que pretenda partilhar recursos, cada colaborador deverá ativar o controlo de acessos através do par utilizador/palavra-chave;
- h) Cada colaborador, não deverá permitir o acesso anónimo via FTP, TFTP, ou qualquer outro tipo de acesso não autenticado a programas ou dados que residam na sua estação de trabalho.

Cópias de segurança

- a) A Friemo,SA assegura a realização de cópias de segurança à informação constante nos servidores. Os dispositivos de cópia de segurança deverão ser etiquetados e protegidos contra o acesso não autorizado;
- b) É da responsabilidade de cada colaborador salvaguardar ficheiros de trabalho nas áreas de arquivo do servidor ou aplicações e não no disco local da sua estação de trabalho;
- c) Não é realizada cópia de segurança à informação constante nas estações de trabalho dos colaboradores quando armazenada no disco local e não nos servidores ou onedrive/sharepoint.

Controlo de acessos

- a) Os visitantes das instalações da empresa, designadamente parceiros, clientes, fornecedores, consultores, candidatos, formadores, representantes, estafetas ou outros convidados deverão entrar nas instalações da empresa, única e exclusivamente, com autorização expressa da pessoa que os irá receber;
- b) Os visitantes deverão indicar o seu nome, motivo da visita e o nome da pessoa que os receberá, sendo que a sua entrada apenas será permitida mediante confirmação e autorização da pessoa indicada como anfitrião;
- c) É proibida ainda a deslocação de pessoas estranhas à organização dentro das instalações e que estejam desacompanhadas;
- d) Durante a visita, os visitantes deverão estar sempre acompanhados do seu anfitrião;

- e) A entrada de visitantes na fábrica, sem autorização e sem o equipamento de segurança é proibida.

Comunicações internas e externas

Para além das boas práticas a observar na utilização da internet, os colaboradores deverão observar algumas regras no que respeita a comunicações internas, entre colaboradores ou empresas do grupo, e externas, com pessoas ou entidades externas, fora da nossa Organização. São elas:

- a) Não divulgar a extensão telefónica, e-mail e telemóvel de um colega sem que este o permita;
- b) Quando falar ao telefone ter cuidado para não divulgar informação confidencial ou, alternativamente, deslocar-se para local ou sala reservada onde possa ser assegurada a confidencialidade da conferência telefónica ou reunião;
- c) Evitar falar de assuntos de trabalho em locais e transportes públicos;
- d) Evitar ler informações críticas de negócio em locais e transportes públicos;
- e) Evitar abrir envelopes com dados confidenciais em espaços públicos;
- f) Evitar utilizar redes sociais ou ferramentas (APPS) públicas para comunicar informação confidencial com parceiros, fornecedores e colegas de trabalho;
- g) Não colocar informações da organização em sites públicos;
- h) Não registar o endereço de e-mail de trabalho em redes sociais;
- i) Não é permitido enviar dados da organização para e de e-mails pessoais;
- j) Pensar nas consequências antes de publicar qualquer informação (uma informação embaraçosa pode comprometer a imagem do colaborador e a da organização).

Segurança e Pagamentos Eletrónicos

Empresas certificadas, como por exemplo as que têm certificação PCI DSS (Payment Card Industry Data Security Standards) são mais seguras nos pagamentos eletrónicos. Isto quer dizer que cumprem as regras de segurança e executam procedimentos que garantem a transação segura de pagamentos eletrónicos.

Para impedir situações de manipulação e fraude com meios de pagamento, devem ser adotadas as seguintes medidas, pelos colaboradores devidamente autorizados, ao abrigo das suas funções, a operacionalizarem pagamentos com os meios de pagamento das empresas:

- a) Observar com atenção o estado do Terminal de Pagamento Automático (ATM), se identificar um teclado diferente mais elevado ou com a ranhura de leitura de cartões alterada, deverá escolher outro ATM;
- b) Comprar apenas em websites seguros e de confiança;
- c) Os websites devem ter mecanismos de segurança tais como: recurso a certificados SSL, tecnologia SET, entre outros;
- d) Utilizar preferencialmente cartões de crédito pré-pagos e carregados com o valor necessário para a compra;
- e) Evitar fazer compras em websites fora da União Europeia;
- f) Especial cuidado com as compras realizadas através de redes WI-FI públicas, muitas destas redes não são seguras e podem estar a guardar os dados dos cartões;
- g) O Departamento Financeiro & Corporativo e as demais áreas funcionais que o integram deverão, quando tais funções lhe sejam atribuídas, consultar os extratos das contas bancárias e de serviços com regularidade. Comunicar imediatamente algum movimento anormal, movimentos não autorizados ou situações fraudulentas, ao prestador de serviço ou à entidade bancária;

Dispositivos Móveis

Os equipamentos móveis são uma potencial fonte de perda de informação crítica de negócio e pessoal. Por este motivo, devem ser tratados com especial atenção e devem estar sempre protegidos. Os colaboradores devem analisar os dispositivos móveis (telemóvel, portátil, *PEN*, pasta de documentos) que têm à disposição e verificar se nos mesmos estão aplicadas algumas das seguintes regras de segurança. São elas:

- a) Todos os dispositivos portáteis devem estar protegidos com password;

- b) Os dispositivos portáteis devem ter os dados encriptados sempre que tal seja tecnicamente possível;
- c) O software deve estar atualizado.
- d) O equipamento deve ter um antivírus instalado e uma firewall;
- e) Devem ser feitas cópias de segurança dos dados. Os dados da organização devem ser colocados nas pastas da rede;
- f) Em locais públicos e transportes públicos os equipamentos devem estar sob vigilância;
- g) O trabalho com equipamentos móveis em locais públicos deve garantir que os dados do ecrã estão protegidos contra pessoas não autorizadas;
- h) Os equipamentos móveis não devem ser deixados nos veículos automóveis;
- i) É expressamente proibido desbloquear equipamentos com recurso a ferramentas ou sistemas operativos não autorizados (ex. *Jailbreak* ou *Root*);
- j) Todos os dispositivos móveis de trabalho que são levados para o exterior da Organização devem estar protegidos contra acesso indevido.

Admissão de colaboradores

Antes da entrada de qualquer colaborador, o serviço de TI deve ser informado com uma antecedência de duas semanas para conseguir proporcionar todas as condições para o correto funcionamento dos equipamentos, para uma correta alocação de licenças e para uma boa atribuição de permissões.

Deve ser enviado por email uma comunicação, onde se reportam as seguintes informações:

- a) Nome;
- b) Função;
- c) Necessidades de software específico (Ex. Autocad, Inventor, etc.);
- d) Permissões para as partilhas de ficheiros.

Saída de colaboradores

Assim que exista a previsão da saída de um colaborador, o serviço de TI deve ser informado para, de acordo com as normas e as boas práticas inativar os acessos desse colaborador e remover as licenças desnecessárias para que a organização consiga gerir os recursos da forma mais eficiente possível.