REGULAMENTO INTERNO DE SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

e

MANIPULAÇÃO DE DADOS

MAVIGRADE UNIP.LDA

25/05/2018

INTRODUÇÃO

O presente Regulamento tem como objectivo estabelecer directrizes e regular a utilização dos recursos informáticos, manipulação de informações, bem como atribuir responsabilidades e definir direitos e deveres dos utilizadores dos sistemas de informação da EMPRESA. Pretende igualmente gerir expectativas de acesso e utilização, restrições e penalidades, assim como contribuir para a criação de uma verdadeira cultura educativa no que diz respeito à utilização e protecção da informação digital da EMPRESA.

Designa-se neste regulamento por "EMPRESA", a MAVIGRADE com actividade FABRICO DE PORTAS,GRADES METALICAS E AUTOMATISMOS,LDA e contribuinte NIF 507 221 214

São objectivos deste regulamento, designadamente:

a) Normalizar as actividades de segurança para o uso e administração dos recursos da infra-estrutura tecnológica da EMPRESA;

b) Fornecer suporte às actividades de segurança que visem garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações;

c) Assegurar que os recursos humanos e tecnológicos envolvidos no manuseamento e processamento da informação estão em conformidade com as regulamentações em vigor.

Artigo 1.º

Definições

Para fins deste Regulamento entende-se por:

a) «UTILIZADOR», funcionários com vínculo contratual à EMPRESA, ou postos à disposição da EMPRESA por entidades externas em regime de colaboração, não importando o regime jurídico a que estejam submetidos, prestadores de serviços que, de qualquer forma, estejam alocados na prestação de serviços, por força de contrato e colaboradores em geral que, directa ou indirectamente, utilizem os sistemas de informação da EMPRESA para o desenvolvimento das suas actividades profissionais;

b) «INFORMAÇÃO», a informação digital ou não, que pode ser de carácter estratégico, técnico, financeiro, legal, de recursos humanos, ou de qualquer outra natureza, não importando se protegida ou não por normas de confidencialidade, desde que se encontre armazenada e/ou manuseada na infra-estrutura tecnológica da EMPRESA e que se constitui como património da EMPRESA;

c) «SEGURANÇA DA INFORMAÇÃO», a adopção de medidas eficazes para garantir que a informação da EMPRESA seja conhecida e manuseada apenas por aqueles que devem conhecê-la, evitando o seu uso indevido, inadequado e/ou ilegal;

d) «REDE INTERNA, REDE EXTERNA, CLOUD, HARDWARE E SOFTWARE», todos os equipamentos ou dispositivos, locais ou não, tais como: computadores "desktop", "notebooks", "Tablets ou Smartphones", servidores, discos ou memórias de armazenamento, equipamentos activos de rede (routers, switchs e hubs, firewalls, proxies), impressoras, digitalizadores, ou qualquer outro equipamento pertencente à infra-estrutura tecnológica da EMPRESA, assim que todo o software licenciado ou estipulado para utilização;

Artigo 2.º

Compromisso dos utilizadores

1. O presente Regulamento de Utilização e Segurança constitui um conjunto de normas de utilização e regras de segurança da informação com o intuito de possibilitar o processamento, partilha e armazenamento de informação da EMPRESA, através do recurso à sua infra-estrutura tecnológica.

2. Os utilizadores são responsáveis, por cumprir, e fazer cumprir, as regras, normas e procedimentos estabelecidos no presente Regulamento.

Artigo 3.º

Gestão do processo de segurança da informação – RGPD

1. Os corpos gerentes desta EMPRESA serão a entidade que assume o cargo de **DPO** (Data Protection Officer) e respetivo serviço de supervisão do cumprimento, pelos utilizadores, das regras do Regulamento.

2. O DPO complementa-se com o responsável Informático e serão responsáveis pela adopção de medidas técnicas que garantam a criação do ambiente tecnológico indispensável para a implementação das normas de segurança, pela análise de todas as infracções cometidas pelos utilizadores (voluntária ou involuntariamente) ao presente regulamento, devendo adoptar as medidas técnicas necessárias para eliminar focos de não conformidade, bem como alertar superiormente para procedimentos irregulares e voluntários dos utilizadores com vista à tomada de medidas correctivas apropriadas.

3. O DPO e o responsável Informático poderão ser contactados, a qualquer momento, pelos utilizadores para esclarecer dúvidas, obter orientações, expressar opiniões ou sugestões, reportar situações de violação ao presente Regulamento e outros.

4. São também atribuições do DPO a divulgação do presente Regulamento.

5. A implementação de novos Sistemas e/ou Aplicações Informáticas poderão conduzir a alterações ao presente Regulamento, se tal se justificar.

Medidas específicas sobre o RGPD – Regulamento Geral de Protecção de Dados

1. O utilizador não deve reunir dados pessoais em papel ou em formato electrónico sem informar o DPO;
2. São dados pessoais todas as informações relativas a uma pessoa identificada ou identificável (nome, morada, património, vencimento, datas, números de cartões, nº de telefone, IP, vídeos, imagem, raça, dados biométricos, folhas de presença, avaliações, curriculum vitae, etc);
3. Cuidado ao enviar dados pessoais, estes devem estar sempre encriptados ou protegidos;
4. Cuidado ao destruir ou eliminar dados pessoais, estes devem ser definitivamente apagados ou eliminados de forma a não serem recuperados por terceiros;
5. Cuidado com os dados pessoais que troca com os seus parceiros e em especial com parceiros fora da EU;
6. Documentos com dados médicos, e dados de menores são muitos sensíveis pelo que deve ter um cuidado redobrado na sua utilização;
7. Se perder ou roubarem dados pessoais informar de imediato o DPO; O DPO tem a obrigação de comunicar às autoridades todas as “fugas” ou perdas de dados pessoais;

Artigo 4.º

Uso da infra-estrutura informática

1. Considerando que a utilização da infra-estrutura tecnológica da EMPRESA é fundamental para o desenvolvimento das actividades profissionais dos seus utilizadores, a mesma é disponibilizada exclusivamente como ferramenta de trabalho.

2. Toda a infra-estrutura informática está sujeitos à monitorização e, portanto:

a) A EMPRESA poderá manter, a seu critério, o histórico de acessos realizados aos seus sistemas;

b) Não é permitida a utilização dos postos de trabalho para armazenar dados e documentos pessoais dos utilizadores (entendidos como aqueles que não são de interesse, uso ou propriedade da EMPRESA);

c) Os dados constantes nas Bases de Dados utilizadas pelos diversos sistemas aplicacionais em utilização pela EMPRESA e, portanto, sua propriedade, devem ser mantidos íntegros e inviolados.

Artigo 5.º

Direitos de acesso à internet

1. O acesso à internet (páginas, sítios e portais) da infra-estrutura informática da EMPRESA está sujeito a monitorização e filtragem.

2. Existe uma aplicação responsável por analisar conteúdos que, dependendo da forma como estão catalogados, poderão ou não ser acedidos.

Artigo 6.º

Receção, inserção e envio de arquivos

1. Ficam estabelecidas as seguintes regras para RECEPÇÃO e INSERÇÃO de ficheiros na infraestrutura informática da EMPRESA, por qualquer meio eletrónico, sem prejuízo de futuras regras que venham a ser definidas pela EMPRESA:

a) Apenas será permitida a recepção de ficheiros para fins de carácter profissional, necessários ao exercício das actividades dos serviços e/ou utilizadores;

b) Está estritamente proibido o carregamento de qualquer arquivo de programas ou scripts executáveis pelos utilizadores, ou outras que possam comprometer o sistema através da execução de comandos maliciosos, sem a permissão da EMPRESA;

2. Apesar da infra-estrutura informática da EMPRESA estar protegida por diversos sistemas contra Vírus e "Worms", "Malware", "Ransomware", incluindo "Spyware" e "Adware", IDS (Detecção de intrusões), IPS (protecção contra acessos não autorizados), etc., fica vedada a INSERÇÃO ou DISSEMINAÇÃO voluntária e intencional, de ficheiros que contenham vírus ou qualquer espécie de programa nocivo, sob pena de responsabilização civil e criminal, de acordo com a legislação em vigor.

3. No tocante ao ENVIO ou RECEÇÃO de ficheiros, através de e-mail, memórias externas (Discos USB, "Pendrives", Cartões de Memória, etc) ou qualquer outra modalidade, fica estabelecido o seguinte conjunto de regras:

a) É proibido o envio de qualquer ficheiro de desenvolvimento, tal como: imagens, textos e/ou códigos-fonte, ficheiros de trabalho, aplicações ou similares, quando o seu envio configurar desrespeito às normas de direitos autorais, ou quaisquer outras normas vigentes no momento do envio do ficheiro;

b) É proibido o envio de qualquer informação resultante da actividade dos serviços, quando esta esteja revestida de confidencialidade, salvo devida autorização superior;

c) É proibido o envio de quaisquer arquivos que violem direitos de terceiros, ou que possam causar prejuízos, a terceiros e/ou à EMPRESA;

d) É proibido o envio de qualquer arquivo com conteúdo que configure prática de infracção penal ou ilícito civil;

e) É proibido o envio de qualquer arquivo de carácter ilegal, ofensivo e/ou imoral, de forma genérica.

4. Caso seja constatado o envio de qualquer arquivo elencado nos tópicos anteriores, os utilizadores responsáveis por tal, podem ficar sujeitos às penalidades previstas na Legislação em vigor, nomeadamente as Leis de Protecção de Direitos de Autor, Lei de Software, Lei da Criminalidade Informática, ou outras que se apliquem aos factos que se venham a apurar.

Artigo 7.º

Software

1. A EMPRESA disponibiliza aos seus utilizadores um conjunto de aplicações informáticas para o desempenho da sua actividade profissional.

2. Estas aplicações ou sistemas aplicacionais, quando não sejam de utilização livre ("freeware"), estão devidamente licenciados para uso interno, através de contratos de licenciamento ou licenças avulsas, sendo vedada a utilização de quaisquer softwares não autorizados pelo responsável informático da EMPRESA encarregue da gestão do licenciamento das aplicações e sua instalação.

3. Desta forma, os utilizadores estão, impedidos de instalar qualquer tipo de aplicação informática, exceptuando-se aqueles que terão permissão expressa, em razão do seu cargo, sem prejuízo pelo respeito da legislação em vigor sobre a protecção dos direitos de autor.

4. Assim, se no caso de, por uma vulnerabilidade do sistema ou por qualquer outro motivo, o utilizador violar esta norma, poderá ser responsabilizado por quaisquer penalidades que a EMPRESA venha a contrair, movidas pelos titulares dos direitos autorais de tais programas não autorizados, bem como de qualquer outra obra intelectual violada nos seus direitos autorais.

5. Os programas informáticos licenciados ou que venham a ser licenciados em nome da EMPRESA são instalados e configurados pela equipa técnica designada pela EMPRESA, ou, em casos pontuais e devidamente justificados, por algum utilizador por ela delegado.

Artigo 8.º

Hardware

1. A EMPRESA disponibiliza aos seus utilizadores um conjunto de equipamentos e máquinas exclusivamente para o desempenho das suas funções e actividades profissionais, sendo o uso inadequado desses equipamentos, para fins que não sejam os delineados pela EMPRESA, proibido.

2. A utilização de quaisquer equipamentos que não sejam de propriedade da EMPRESA, para conexão à sua infra-estrutura informática, especialmente os computadores portáteis, "PDA's", "smartphones" ou outros, e uma vez que comprometem a Segurança da Informação, deve ser solicitada ao responsável Informático, que procederá à normalização e configuração da máquina em questão.

3. Durante a utilização dos computadores e periféricos, propriedade da EMPRESA, o utilizador deverá observar os seguintes cuidados:

a) Terminar a sessão e/ou desligar os equipamentos no final do expediente, ou em ausências prolongadas;

b) Sempre que se ausentar do local de trabalho deve terminar a sessão ou bloquear a mesma;

c) Sempre que tiver dúvidas ou problemas nos equipamentos, o utilizador deve contactar o responsável Informático;

4. A alteração de qualquer periférico ou componente nos equipamentos não é permitida, ficando vedada aos utilizadores. A realização de qualquer modificação ou manutenção deverá sempre ser efetuada pela área de suporte técnico da EMPRESA.

Artigo 9.º

Equipamentos portáteis

1. Os equipamentos portáteis, designadamente computadores portáteis "notebooks", "smartphones", "PDAs", e quaisquer outros que permitam armazenamento de dados e informações, propriedade da EMPRESA, estarão devidamente configurados para conexão à infra-estrutura informática da EMPRESA e devem ser utilizados exclusivamente para as funções profissionais a que foram adstritos.

2. Desse modo, a utilização de equipamentos portáteis particulares está vedada, salvo os casos excepcionais, que carecem de autorização superior e cuja configuração deverá ser executada pelo responsável Informático. No entanto, deve o utilizador ficar ciente que não é permitida a cópia e/ou transferência de informações ou dados de propriedade desta EMPRESA através destes equipamentos, bem como zelar pela segurança dos dados e/ou aplicações nos mesmos armazenada, nomeadamente não deixar esses equipamentos fora do alcance em locais públicos, onde haja acesso de múltiplas pessoas, bem como, não permitir que terceiros não autorizados tenham acesso às informações ou dados transportados nesses equipamentos.

Artigo 10.º

Equipamentos de impressão digital

1. O uso das impressoras ou qualquer outro equipamento de impressão digital, deve ser feito exclusivamente para impressão de documentos ou outras informações que sejam de interesse da EMPRESA ou que estejam relacionados com o desempenho das atividades inerentes às funções que o utilizador desempenha na organização.

Artigo 11.º

Procedimentos para o uso da internet

1. Sendo o acesso a redes externas, nomeadamente a Internet, fundamental para o desempenho de algumas actividades relacionadas com as competências de cada serviço da EMPRESA, a utilização da Internet deve estar voltada para o acesso às informações e/ou plataformas "web" relacionadas essas mesmas actividades.

2. A navegação em sites não relacionados directamente com a actividade laboral do utilizador, não é proibida, porém seu uso deve ser feito de maneira equilibrada e responsável, para assegurar à EMPRESA a máxima segurança e performance no trabalho.

3. A utilização de Redes Sociais nas infra-estruturas tecnológicas da EMPRESA deve ser devidamente/previamente autorizada pelo DPO ou responsável informático.

4. Sem prejuízo do disposto no parágrafo anterior, e estando todo o tráfego sujeito a monitorização e filtragem, pode ser bloqueada, com grande percentagem de confiança, a navegação nos sites com a seguinte catalogação:

- Pornografia de qualquer tipo;
- Partilha de ficheiros (ex.: peer to peer);
- Terrorismo;
- Drogas;
- Hackers e qualquer tipo de pirataria informática;
- Jogos;
- Violência e agressividade (racismo, xenofobia, etc.);
- Vídeo e Áudio, exceptuando-se os de interesse para a EMPRESA, ou para as funções desempenhadas pelo utilizador em questão;
- Música on-line;
- Outros, que se considerem desadequados para as funções do utilizador.

5. Apesar de se tratar de um sistema que se baseia numa base de dados, atualizada diariamente, onde estão catalogados vários milhões de páginas Web, a ocorrência de falsos positivos deve ser reportada ao responsável Informático, que procederá à análise e desbloqueio do endereço em questão.

Artigo 12.º

Correio eletrónico (e-mail)

1. O e-mail é uma ferramenta de trabalho cada vez mais vulgarizada e utilizada. Por esse motivo é disponibilizado, 24h por dia, a todos os utilizadores, e deve ser utilizado no âmbito das funções desempenhadas na EMPRESA.

2. O DPO e o responsável informático são responsáveis pela oportunidade, definição e criação desses endereços.

3. Todo e qualquer e-mail enviado por utilizadores da EMPRESA, deverá conter, no final da mensagem, uma assinatura padrão, de acordo com o seguinte modelo:

<Nome>
NOME EMPRESA
www sitewebempresa com
<Telefone>
<Fax>

4. Após a assinatura padrão, deverá conter o seguinte aviso:

AVISO DE CONFIDENCIALIDADE
Esta mensagem de correio electrónico e qualquer dos seus ficheiros anexos, caso existam, são confidenciais e destinados apenas à(s) pessoa(s) ou entidade(s) acima referida(s), podendo conter informação privilegiada, a qual não deverá ser divulgada, copiada, gravada ou distribuída nos termos da lei vigente. Se não é o destinatário da mensagem, ou se ela lhe foi enviada por engano, agradecemos que não faça uso ou divulgação da mesma. A distribuição ou utilização da informação nela contida NÃO É AUTORIZADA. Se recebeu esta mensagem por engano, por favor avise-nos de imediato, por correio electrónico, para o endereço acima e apague este e-mail do seu sistema. Obrigado.

5. Fica estabelecida a seguinte política com relação ao uso de e-mail:

a) A conta de e-mail, fornecida pela EMPRESA deverá ser utilizada para o envio e recepção de mensagens relacionadas com os trabalhos desenvolvidos pelos utilizadores no âmbito das suas funções nesta EMPRESA. O utilizador está ciente que o conteúdo está ou pode estar sujeito a monitorização e filtragem;

b) Fica proibido o envio de todo e qualquer tipo de e-mail com conteúdo impróprio ou pornográfico e afins bem como qualquer tipo de mensagem que possa prejudicar o trabalho de terceiros, causar excessivo tráfego na rede e/ou sobrecarregar a infra-estrutura tecnológica da EMPRESA;

c) A conta de e-mail não deverá ser utilizada para disseminar ou transmitir informações que violem a legislação em vigor, tais como ameaças, difamação, calúnia, injúria, racismo, pornografia infantil, etc..

6. O utilizador fica ciente da inexistência de expectativa de privacidade na utilização da sua conta de e-mail corporativa, bem como na navegação em sites da internet, efetuada através da infra-estrutura tecnológica da EMPRESA. Fica ainda ciente da existência de sistemas de monitorização e filtragem de conteúdos, quer nas mensagens, quer na navegação na internet.

7. A filtragem e monitorização do tráfego descrito neste Regulamento tem por objectivo garantir o respeito dos utilizadores pelas regras estabelecidas no presente instrumento, bem como proteger toda a infra-estrutura de ameaças à Segurança da Informação nela contida.

8. A monitorização será realizada, a qualquer momento e de forma automática, através da utilização de diversos sistemas informáticos existentes para tal finalidade e mantidos na infra-estrutura tecnológica desta EMPRESA. Na sequência de tal monitorização e/ou filtragem, as mensagens enviadas para um e-mail da EMPRESA poderão ser redireccionadas para outro e-mail interno, na sequência de suspeita de conter conteúdo malicioso que ponha em causa a segurança da informação, sem necessidade de qualquer aviso prévio e sem conhecimento do emissor e do receptor da mensagem.

9. Em casos pontuais e por solicitação ou necessidade especifica de um qualquer serviço, poderão ser criadas contas de e-mail por serviço, partilhadas por vários utilizadores, que deverão respeitar as regras em vigor para as contas de e-mail por utilizador.

Artigo 13.º

Acesso a contas de e-mail particulares

1. Caso o utilizador tenha acesso a sites de e-mail (gratuitos ou pagos), que disponibilizem a consulta, envio e recepção correio electrónico através da tecnologia “webmail”, fica ciente que tal acesso pode comprometer a segurança da informação da EMPRESA, motivo pelo qual deve ser efetuado com cautela e moderação.

2. Além disso, considerando que os e-mails pessoais acedidos através da infra-estrutura tecnológica da EMPRESA, serão realizados através da conexão à Internet pertencente à mesma, vinculado a um endereço IP Público Fixo ou não, a sua utilização indevida poderá gerar responsabilidades à EMPRESA. Por isso se justifica a necessidade de maior cautela por parte dos utilizadores.

3. Como resulta óbvio da constante neste documento, é vedado o envio de informações, dados ou ficheiros, propriedade da EMPRESA e que ponham em risco a segurança e confidencialidade da informação. Destes casos se exceptuam aqueles em que haja necessidade absoluta ou autorização específica, devendo ser garantido, no entanto, o uso dentro dos normais padrões de segurança.

NORMAS E PROCEDIMENTOS GERAIS

Artigo 14.º

Confidencialidade

Todas as informações internas, obtidas na execução de suas actividades no âmbito funções que detêm ou detiveram na EMPRESA, deverão ser tratadas pelos utilizadores como sigilosas e restritas, não as devendo divulgar a terceiros, mesmo que o vínculo contratual que o possa ter vinculado a esta Instituição tenha terminado, independentemente da forma como tenha ocorrido.

Artigo 15.º

Manuais, suportes e licenças

Os manuais, suportes lógicos (CD's, DVD's, etc) e licenças da infra-estrutura tecnológica adquiridos pela EMPRESA são para utilização dos utilizadores durante a realização das suas actividades profissionais, ficando assim sob a sua responsabilidade o perfeito estado, organização e guarda.

Artigo 16.º

Suporte técnico

Será disponibilizado, pelo serviço de informática da EMPRESA ou qualquer equipa técnica contratada para o efeito, a todos os utilizadores, suporte técnico ao uso dos recursos informáticos disponibilizados pela EMPRESA.

Artigo 17.º

Guarda de logs e auditoria

Todas as actividades desenvolvidas com a utilização da infra-estrutura tecnológica da EMPRESA poderão, a seu critério, ser registadas para eventual análise ou auditoria, por um período até 12 (doze) meses. Essas actividades incluem acesso à rede, informações, "logs" de manuseamento de bases de dados, "logs" de envio e recepção de correio electrónico, acesso e navegação a sites, etc.

Artigo 18.º

Casos omissos

Os casos omissos neste Regulamento deverão ser encaminhados aos corpos gerentes da EMPRESA para avaliação e posterior regulamentação, bem como para recomendação de medidas a tomar pelo Executivo, quando for caso disso.