

# A SEGURANÇA DA INFORMAÇÃO

## Informação ao Colaborador





# Índice

|  |    |
|--|----|
| Introdução .....                                   | 1  |
| Princípios gerais de segurança da informação ..... | 2  |
| As <i>passwords</i> e o acesso à informação .....  | 3  |
| Posto de trabalho e salas de reuniões .....        | 4  |
| O correio eletrónico e NetEtiqueta .....           | 5  |
| <i>Phishing</i> , vírus e <i>ransomware</i> .....  | 6  |
| A Internet e a comunicação .....                   | 7  |
| Dispositivos móveis .....                          | 8  |
| Parceiros externos .....                           | 9  |
| RGPD .....   | 10 |
| Destruição de dados e impressões .....             | 11 |
| Segurança de pagamentos eletrónicos .....          | 12 |

# Introdução

## O que é a segurança da informação?

É um processo organizado e estruturado que permite preservar a confidencialidade, integridade e a disponibilidade da informação.

**Confidencialidade é...** assegurar que a informação é acessível somente por pessoas devidamente autorizadas. O acesso à informação é restrito a utilizadores legítimos.

**Integridade é...** garantir a veracidade e complementaridade da informação, bem como os seus métodos de processamento. O conteúdo da informação não pode ser modificado de forma inesperada.

**Disponibilidade é...** assegurar o acesso à informação e bens associados por quem devidamente autorizado. A informação deve estar acessível sempre que necessário.



## Quem é o responsável pela segurança da informação?

Todos nós somos responsáveis pela segurança da informação e todos temos a responsabilidade de proteger os nossos dados e os que nos são confiados.

No entanto, as organizações possuem pessoas especializadas e dedicadas à segurança da informação e à proteção dos dados pessoais.

Estes colaboradores são normalmente designados por CISO - *Chefe Information Security Officer* ou por DPO - *Data Protection Officer*. São responsáveis pela proteção da informação contra quebras de confidencialidade, integridade e disponibilidade da mesma.

As principais tarefas do CISO são:

- Implementar boas práticas de segurança de informação holísticas e estruturadas (Ex. CISO, COBIT, ITIL, etc.);
- Aplicar, contribuir e rever as normas, políticas e *standards* de segurança de informação;
- Executar auditorias e controlos internos regulares;
- Realizar ações de sensibilização e de formação para os utilizadores;
- Apoiar a organização e em especial o IT e os gestores de projeto, com foco na segurança;
- Colaborar na estratégia, desempenho e monitorização do IT.

Para que esta função tenha sucesso a colaboração e o envolvimento de todos é fundamental. Conto com a tua ajuda!

Assim como, sempre que necessitares, o CISO está disponível para te ajudar.





# Princípios gerais de segurança da informação

A proteção eficaz e adequada da informação e dos sistemas de informação contra quebras de confidencialidade, de integridade e de disponibilidade garante a capacidade de produção e a posição concorrencial da organização, a confiança junto dos clientes e parceiros, bem como a imagem junto do público, faz parte imprescindível da política da organização.

- Estamos cientes da elevada importância da segurança da informação para a nossa organização e tratamo-la de forma adequada;
- Implementamos procedimentos sistemáticos que visam a redução dos riscos;
- Incutimos a responsabilidade pela segurança da informação;
- Estabelecemos medidas adequadas à nossa organização para garantir a segurança da informação. Verificamos regularmente o respetivo cumprimento e a eficácia;
- Protegemos a informação própria e a que nos é confiada, impedindo a sua divulgação e alteração ilegal;
- Reagimos de imediato e adequadamente à situação em caso de violação da segurança;
- Garantimos a disponibilidade dos sistemas de informação com base nas exigências dos processos de negócio;
- Implementamos procedimentos adequados à não interrupção da atividade;
- As regras de segurança da informação são afixadas e comunicadas aos colaboradores, fornecedores e parceiros.

Password:

\*\*\*\*\*



# As *passwords* e o acesso à informação

As organizações estão dotadas de políticas, processos, *standards* e guias de orientação.

O principal objetivo é garantir a segurança dos dados confidenciais de negócios e dados pessoais.

Algumas dicas de segurança:

- Mantém as tuas *passwords* confidenciais;
- Memoriza as tuas *passwords*. As *passwords* não devem ser escritas em papéis ou locais visíveis;
- Muda as tuas *passwords* regularmente, mesmo nos sistemas que não te obriguem a fazê-lo;
- Guarda as tuas *passwords* em *softwares* encriptados (ex. KeePass Safe);
- Respeita a política de *passwords*;

- Não graves as tuas *passwords* de forma automática nos sistemas;
- Não utilizes as mesmas *passwords* para os sistemas da organização e sistemas pessoais;
- Utiliza *passwords* seguras mas fáceis de memorizar.

| As <i>passwords</i> mais utilizadas são:                                       | Como criar <i>passwords</i> seguras:  |
|--|---|
| 1ª 123456;<br>2ª Password;<br>3ª qwerty;<br>4ª Abcd1234;<br>5ª Data nascimento | Construa uma frase.<br>O meu filho nasceu em Lisboa às 18:35!<br><br><b>A <i>password</i>: OmfneLa1835!</b> |

# Posto de trabalho e salas de reuniões

O posto de trabalho é uma “ferramenta” cuidadosamente pensada para que os colaboradores da nossa organização possam trabalhar de forma organizada, confortável e adequada às suas funções.

O teu posto de trabalho é constituído por documentos e ferramentas que fazem parte de uma rede complexa, constituída por milhares de computadores e outros equipamentos.

Implementamos medidas e procedimentos que protegem o teu posto de trabalho, a informação do negócio e os teus dados pessoais.

Todos os colaboradores fazem parte da cadeia de segurança, por isso, para que a nossa informação esteja protegida a tua colaboração é fundamental.

## Posto de trabalho

O teu posto de trabalho deve estar sempre arrumado e cumprir o princípio “*clean desk*”.

Não é permitido ligar equipamentos elétricos tais como ventoinhas, aquecedores, etc.

Durante as reuniões, com temas confidenciais ou sensíveis, deves verificar se a sala está corretamente fechada e protegida para que a informação seja partilhada de forma confidencial.

No fim do dia de trabalho deves verificar se as portas e janelas ficaram corretamente fechadas.



## O PC

Quando não estás a utilizar o teu computador bloqueia a tua sessão.



O teu PC apenas tem *software* autorizado e devidamente licenciado.

Evita o armazenamento de dados em pastas locais, todos os documentos de trabalho devem estar armazenados nas pastas da rede.

## Documentos

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.

Sempre que te afastes do teu posto de trabalho coloca os documentos dentro de armários ou gavetas devidamente trancadas.

As impressões devem ser recolhidas da impressora o mais rápido possível.

Quando imprimes documentos confidenciais deves acompanhar presencialmente a saídas das folhas e garantir que foram todas recolhidas da impressora.





# O correio eletrónico e NetEtiqueta

O correio eletrónico (email) 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 nossos sistemas e à nossa informação.

## Boas práticas de utilização do email:

1. Utiliza o email de forma segura, produtiva, profissional e educada;
2. Não reenvies emails com brincadeiras ou correntes da fortuna e felicidade nem reajas por impulso ao conteúdo;
3. Verifica sempre os endereços dos destinatários;
4. Não abras emails e ficheiros de origem desconhecida, elimina-os imediatamente;
5. Nunca envies informação pessoal que te seja solicitada por email, tal como: n.º do cartão de crédito, *username*, *password*, nomes. Nenhuma empresa te pedirá este tipo de informação por email;
6. Não sigas as ligações (*links*) de emails suspeitos. Escreve o endereço diretamente no *browser*;
7. Informações críticas de negócio ou dados pessoais só podem ser enviados em formato encriptado. As *passwords* devem ser enviadas por outro meio de comunicação.

## NetEtiqueta

- Evita escrever mensagens em MAIÚSCULAS com cores e a **bold**;
- Tenta ser claro e objetivo, produz textos simples e com cuidado gramatical e ortográfico;
- Tenta ser educado e simpático, agradece e cumprimenta;
- Podes usar *smileys* :-)) é uma forma simples de dar a entender os teus sentimentos;
- Não reajas de forma emotiva porque normalmente escrevemos emails ou partilhamos o que não queremos;
- Antes de publicar alguma informação verifica se o conteúdo:
  - Tem interesse;
  - Tem qualidade, é atual e respeita a missão da organização;
  - Tem o formato correto e está a ser publicado no dia, hora e local correto.



# Phishing, vírus e ransomware

O **Phishing** é uma das principais preocupações ao nível da segurança da informação. Trata-se de um crime informático baseado no envio de um e-mail fraudulento com o objetivo de obter dados pessoais ou de negócio. É um e-mail falso, normalmente emitido em nome de uma entidade credível tal como um Banco, Facebook, Twitter, Microsoft, Vodafone, etc. mas que na realidade só pretende recolher dados ou infetar os sistemas.

## Vírus

Os vírus são programas maliciosos - *malware*; que se espalham a outros computadores com o objetivo de permitir acessos ou danificar dados e serviços.

Existem diferentes tipos de vírus: o *spyware* que regista a atividade do utilizador e envia para o atacante; o *adware* que ataca o utilizador com publicidade; o *scareware* que é um falso alerta de vírus ou problemas informáticos que levam o utilizador a fazer o que lhe pedem, por como exemplo instalar um programa; e o *ransomware*, um dos mais agressivos e de maior impacto.

O **Ransomware** é uma estratégia de resgate suportada por um *software* de encriptação que bloqueia o acesso aos ficheiros ou aos computadores, até que se pague o resgate. Este *software* encripta os dados com uma chave secreta.

## “O teu dinheiro ou os teus dados?”

Para recuperarmos os dados é necessário pagar um resgate.

Normalmente este ataque ocorre em 6 passos:

1. O *ransomware* entra via email ou *download* da internet;
2. O utilizador abre o ficheiro e este executa-se;
3. O *software* gera uma chave pública e uma privada;
4. A chave privada é transferida para um servidor do atacante e é apagada do teu PC;
5. O *software* começa a encriptar os teus dados;
6. Terminada a encriptação o *software* malicioso coloca uma mensagem no *desktop* com instruções para pagares o resgate com Bitcoin.

**NOTA:** Se o teu computador detetar um vírus ou suspeitares de um comportamento anormal por favor segue os seguintes passos:

1. Desliga o *Wi-Fi*;
2. Remove o cabo de rede (ou retira o portátil da *docking station*);
3. Não desligues o equipamento;
4. Contacta imediatamente a equipa IT.

# A Internet e a Comunicação

Vivemos no mundo da informação e a comunicação é a chave do sucesso pessoal e empresarial. Por este motivo é fundamental garantirmos que comunicamos de forma adequada, nos meios adequados e apenas transmitimos a informação necessária.

No mundo da internet existem regras e códigos de conduta com o objetivo de melhorar a segurança da informação.

## Internet

- Certifica-te que o site é seguro fazendo duplo clique sobre o cadeado ou acede pelo endereço (URL) que deve começar por "https://" e não por "http://";
- Certifica-te que o teu *browser* e o antivírus estão atualizados e utiliza uma *firewall* pessoal;
- Consulta os extratos das tuas contas bancárias e de serviços com regularidade. Se encontrares algum movimento estranho, contacta imediatamente o prestador de serviço ou banco;
- Atualiza as tuas *passwords*/PIN a cada 90 dias. Sempre que possível utiliza *passwords* diferentes para sites seguros e sites não seguros;

- Não é permitido aceder a sites com conteúdos ilegais ou inadequados;
- Não é permitido utilizar serviços públicos de email, de transferência de ficheiros e ou serviços *cloud* para troca de dados da organização;
- Não é permitido divulgar informação de negócio nas redes sociais;
- Não é permitido utilizar ferramentas da internet para criar ou traduzir conteúdos (ex. Google Translate ou Prezi);
- Não é permitido jogar ou fazer apostas online com recursos da nossa organização (REDE, PCs, etc.).





## Comunicação

- Não divulgues a extensão telefónica, email e telemóvel de um colega sem que este o permita;
- Quando falas ao telefone tem cuidado para não divulgar informação confidencial;
- Evita falar de assuntos de trabalho em locais e transportes públicos, protege-te contra os ouvintes;
- Evita ler informações críticas de negócio em locais e transportes públicos, protege-te dos mirões;
- Evita abrir envelopes com dados confidenciais em espaços públicos;
- Não utilizes redes sociais ou ferramentas (APPS) públicas para comunicar com parceiros e fornecedores (ex: WhatsApp ou Wunderlist), estas não são seguras;
- Não coloques informações da organização em sites públicos (ex. Dropbox);
- Não registes o teu endereço de e-mail de trabalho em redes sociais;
- Não é permitido enviar dados da organização para e-mails pessoais (Ex. Gmail, Hotmail, etc.);
- Pensa nas consequências antes de publicares qualquer informação, uma informação embaraçosa pode comprometer a tua imagem e a da tua organização.





# 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.

Olha para os teus dispositivos móveis (telemóvel, portátil, *PEN*, *token*, pasta de documentos) e verifica se estão aplicadas algumas das seguintes regras de segurança.

- Todos os dispositivos portáteis estão protegidos com *password*;
- Os dispositivos portáteis devem ter os dados encriptados sempre que seja tecnicamente possível;
- O *software* deve estar atualizado. Sempre que possível liga o teu equipamento à rede da organização para receber as devidas atualizações (pelo menos a cada 15 dias);
- O equipamento deve ter instalado um antivírus e uma *firewall*;
- Devem ser feitas cópias de segurança dos dados. Os dados da organização devem ser colocados nas pastas da rede;
- Em locais públicos e transportes públicos os equipamentos devem estar sob vigilância;
- O trabalho com equipamentos móveis em locais públicos deve garantir que os dados do ecrã estão protegidos contra pessoas não autorizadas;
- Os equipamentos móveis não devem ser deixados nos veículos automóveis;
- O computador portátil deve estar sempre com o cadeado de segurança para evitar roubos;
- É proibido desbloquear equipamentos com recurso a ferramentas ou sistemas operativos não autorizados (ex. Jailbreak ou Root);
- *Home-office* - os documentos que são levados para trabalhar em casa devem estar protegidos contra acesso indevido.



# Parceiros externos

Existe uma ordem cronológica natural de relacionamento com os parceiros externos, esta ordem passa pelas seguintes fases:

1. Antes do contrato;
2. Durante o período de relação de negócio;
3. E terminada a relação de negócio.

Para todas estas fases estão definidas regras e boas práticas que garantem a proteção dos dados, e das infraestruturas da nossa organização e dos nossos parceiros. Estas regras aplicam-se a todos os parceiros externos.

## Antes do contrato:

- Os parceiros e as empresas subcontratadas assinam um NDA - Acordo de Confidencialidade;
- Os parceiros que processam ou armazenam dados da nossa organização recebem um *briefing* de segurança da informação;
- São definidos os dados a serem trocados e os canais seguros para a troca;
- São definidos os interlocutores do parceiro e os nossos, e acordado entre ambos a forma de comunicar incidentes de segurança;

- Se forem trocados dados críticos (pessoais ou de negócio) os interlocutores devem garantir que foram tomadas as medidas de proteção técnicas e funcionais adequadas;
- O prestador de serviço apresenta um plano de segurança claro e atualizado;
- É assinado um contrato-tipo disponibilizado pelo Departamento Jurídico.



## Durante a relação de negócio:

- São atribuídos acessos locais ou remotos aos parceiros de acordo com princípio do “Mínimo acesso permitido”;
- Os sistemas dos parceiros externos apenas podem ser instalados na nossa infraestrutura se existirem comprovadas razões técnicas ou económicas;

- Não é permitido instalar o nosso *software* em equipamentos de parceiros;
- Os nossos sistemas apenas podem ser colocados nas instalações dos parceiros após aprovação formal do CISO;
- Em todos os contratos deve ser assegurado o direito de auditoria aos parceiros e fornecedores, estas auditorias pode ser realizadas por nós ou por um parceiro escolhido pelas partes e acontecem no âmbito da prestação de serviço.



#### **Terminada e relação de negócio:**

- O interlocutor da nossa organização informa todos as entidades envolvidas;
- Todos os privilégios são imediatamente eliminados;
- Todos os equipamentos são desligados e recolhidos.



O novo **Regulamento Geral sobre a Proteção de Dados**, constante do **Regulamento (UE) 2016/679**, foi publicado no Jornal Oficial da União Europeia no dia **4 de maio de 2016**. Este regulamento revoga toda a legislação publicada antes da era digital.

Este normativo comunitário, designado na língua inglesa por **General Data Protection Regulation (GDPR)**, é aplicável a partir do dia **25 de maio de 2018**.

O período de dois anos tem como principal objetivo permitir que as organizações se adaptem às novas regras tais como:

- Novos direitos e obrigações, ex. direito ao esquecimento e a portabilidade dos dados, etc;
- Coimas elevadas em caso de incumprimento, até 20 milhões de euros ou 4% do volume anual de negócios do grupo;
- Incluir a privacidade desde a conceção como princípio orientador (*Privacy by default*);
- A confiança nas TIC, impõe garantir que as tecnologias não afetam os direitos fundamentais das pessoas à privacidade e à proteção dos dados pessoais (*Privacy by Design*);
- Princípio de responsabilidade na recolha e proteção dos dados, *Accountability* e *Opposition to Profiling*;
- Define a criação de uma nova função DPO - *Data Private Officer* que no regulamento português se designa por Encarregado da Proteção de Dados.

É importantes saberes:

- O que são dados pessoais - são 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);
- Não deves reunir dados pessoais em papel ou em formato eletrónico sem informares o DPO;
- Cuidado ao enviarees dados pessoais, estes devem estar sempre encriptados ou protegidos;
- Cuidado ao destruíres ou eliminares dados pessoais, estes devem ser definitivamente apagados ou eliminados de forma a não serem recuperados por terceiros;
- Cuidado com os dados pessoais que trocas com os teus parceiros e em especial com parceiros fora da EU;
- Documentos com dados médicos, e dados de menores são muitos sensíveis pelo que deves ter um cuidado redobrado na sua utilização;
- Se perderes ou te roubarem dados pessoais informa de imediato o teu DPO;
- O DPO tem a obrigação de comunicar as autoridades todas as “fugas” ou perdas de dados pessoais.





# Destruição de dados e impressões

Informação é um ativo com valor para o negócio. A informação pode existir sob várias formas, como por exemplo: em suportes de papel (folhetos, jornais, cartolinas, *posters*, etc.) ou suportes eletrónicos designados por *media* (CDs, disquetes, tapes, microfilme, discos rígidos, *PEN USB*, cartões de memória, etc.).

A destruição de informação confidencial deve ser realizada de acordo com regras de segurança e procedimentos adequados.

**Apenas empresas certificadas podem fazer a destruição da nossa informação.**

**Existe contrato com empresas certificadas para a destruição de informação.**

Estas empresas garantem a recolha e o transporte dos documentos e equipamentos, em condições de rigorosa segurança, através da utilização exclusiva de viaturas próprias com caixa blindada, cumprindo os requisitos previstos na Lei da Proteção de Dados Pessoais e os requisitos associados ao acondicionamento e transporte de resíduos.

1. Existe um contentor para se depositarem todos os suportes de dados digitais para destruição segura.

2. Junto do contentor existe uma pasta com formulário para registar o material colocado no contentor para destruição.

3. Semestralmente a empresa recolhe o contentor e deposita um vazio.

4. No processo de destruição a empresa produz um relatório detalhado com a descrição dos dispositivos, quantidade e código de barras.

5. A documentação e certificados de destruição ficarão à guarda do CISO.

6. A destruição de grandes volumes de papel é feita a pedido.

7. A destruição de pequenos volumes (documentos de trabalho e *flip charts* com informação confidencial) é realizada pelo próprio colaborador nos destruidores de papel disponibilizados pela empresa.

8. A eliminação das impressões deve ocorrer no escritório. No escritório de casa, a eliminação de impressões só é permitida se os documentos forem cortados por uma trituradora de corte em pedaços com o máximo de 8 mm.

9. Os equipamentos eletrónicos *media* só podem ser destruídos ou ter os dados apagados pelo IT.



# Segurança de pagamentos eletrónicos

Empresas certificadas, como por exemplo as que têm certificação PCI DSS 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 recomendamos atenção a:



1. Observe com atenção o estado do Terminal de Pagamento Automático (ATM), se identificares um teclado diferente mais elevado ou com a ranhura de leitura de cartões alterada, escolhe outro ATM;
2. Comprar apenas em websites seguros e de confiança,
3. Os websites devem ter mecanismos de segurança tais como: recurso a certificados SSL, tecnologia SET, entre outros;
4. Utiliza apenas cartões de crédito pré-pagos e carregados com o valor necessário para a compra;
5. Evita fazer compras em websites fora da União Europeia, pois poderás ter problemas em caso de necessidade de reclamar;
6. Cuidado com as compras feitas em redes WI-FI públicas, muitas destas redes não são seguras e podem estar a guardar os dados dos teus cartões.

Sempre que possível utiliza o *contactless*, é a melhor forma de protegeres o teu PIN.

## O que é a tecnologia *Contactless*?

A tecnologia *Contactless* permite rapidez no pagamento. Basta aproximar o cartão a 4 cm do terminal para que a operação de pagamento seja efetuada.

## Como reconheço que o meu cartão é *Contactless*?

Caso o cartão tenha o símbolo  ou  está preparado para efetuar pagamentos em *Contactless*.

## É seguro não introduzir o cartão no terminal e o PIN nos pagamentos abaixo dos 20€?

Sim, porque o pagamento com *Contactless* obedece a todos os critérios de segurança exigidos pelos bancos.

## Há um valor limite para pagamentos via *Contactless*?

Sim, o pagamento de compras *Contactless* está limitado a 20€ sem que seja necessária a introdução do código PIN para validar a compra.

## E em pagamentos acima de 20€ continua a ser possível utilizar o sistema *Contactless*?

Sim, mas será necessário validar a operação com o código PIN, apesar de o pagamento ser efetuado sem introdução do cartão no terminal.

## Nunca mais será necessário introduzir o PIN para compras inferiores a 20€?

Não, o número de transações *Contactless* é limitado. É necessário introduzir o PIN de 4 em 4 transações ou quando seja atingido o montante acumulado de 60€ em pagamentos *Contactless*.

## Quais as vantagens do *Contactless*?

Maior rapidez e segurança no pagamento, menos trocos, mas a principal vantagem é a proteção do teu PIN. Isto é, quanto menos vezes utilizares o teu código PIN mais protegido está o teu dinheiro.

Protege o teu código PIN!!!

**A segurança da informação da nossa  
organização também depende de ti!**

Stand: Outubro/2017 \* José Jorge Vicente - ISO - Lidl PT

