

A SEGURANÇA DA INFORMAÇÃO

INFORMAÇÃO AO COLABORADOR

Novembro | 2017



REPÚBLICA
PORTUGUESA

SAÚDE



SNS SERVIÇO NACIONAL
DE SAÚDE



SPMS
EPE
Serviços Partilhados do Ministério da Saúde



Índice

Introdução 4

Princípios gerais de segurança da informação 7

As *passwords* e o acesso à informação 9

Posto de trabalho e salas de reuniões 10

O correio eletrónico e NetEtiqueta 12

Phishing, vírus e ransomware 14

A Internet e a comunicação 16

Dispositivos móveis 18

Parceiros externos 20

GDPR 22

Destruição de dados e impressões 24

Segurança de pagamentos eletrónicos 26

Dez Mandamentos de Segurança 29

1 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.

Para que esta função tenha sucesso a colaboração e o envolvimento de todos é fundamental. **Contamos com a sua ajuda!**

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

As principais tarefas do CISO são:

- ✓ Implementar boas práticas de segurança da 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, em especial as TIC e os gestores de projeto, com foco na segurança;
- ✓ Colaborar na estratégia, desempenho e monitorização das TIC.



2 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 continuidade da produção da organização, a confiança junto dos utentes 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;
- ✓ Inculcamos 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 legal;
- ✓ 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

3 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 e dados pessoais.

Algumas dicas de segurança:

- ✓ Mantenha as suas *passwords* confidenciais;
- ✓ Não utilize as mesmas *passwords* para os sistemas da organização e sistemas pessoais;
- ✓ Memorize as suas *passwords*. As *passwords* não devem ser escritas em papéis ou locais visíveis;
- ✓ Utilize *passwords* seguras, mas fáceis de memorizar.
- ✓ Mude as suas *passwords* regularmente, mesmo nos sistemas que não obriguem a fazê-lo;
- ✓ Guarde as suas *passwords* em *softwares* encriptados (ex. *KeePass Safe*);
- ✓ Respeite a política de *passwords*;
- ✓ Não grave as suas *passwords* de forma automática nos sistemas;

As *passwords* mais utilizadas são:

- | | |
|-------------|--------------------|
| 1ª 123456 | 4ª Abcd1234 |
| 2ª Password | 5ª Data nascimento |
| 3ª qwerty | |

Como criar *passwords* seguras:

Construa uma frase.
Eu quero um SNS seguro em 2017!

A *password*: EquSNSse2017!

4 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 seu 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 seu posto de trabalho, a informação do negócio e os seus dados pessoais.

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

Posto de trabalho

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

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

O PC

Quando não está a utilizar o seu computador bloqueie a sua sessão.



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

Evite 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 se afaste do seu posto de trabalho coloque os documentos dentro de armários ou gavetas devidamente trancadas.

As impressões devem ser recolhidas da impressora o mais rápido possível. Quando imprime documentos confidenciais deve acompanhar presencialmente a saídas das folhas e garantir que foram todas recolhidas da impressora.





5

O correio eletrónico e NetEtiqueta

O correio eletrónico (e-mail) é uma ferramenta de trabalho que 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 e-mail

1. Utilize o e-mail de forma segura, produtiva, profissional e educada;
2. Não reenvie e-mails com brincadeiras ou correntes da fortuna e felicidade nem reaja por impulso ao conteúdo;
3. Verifique sempre os endereços dos destinatários;
4. Não abra e-mails e ficheiros de origem desconhecida, elimine-os imediatamente;
5. Nunca envie informação pessoal que lhe seja solicitada por e-mail, tal como: n.º do cartão de crédito, *username*, *password*, nomes. Nenhuma empresa lhe pedirá este tipo de informação por e-mail;
6. Não siga as ligações (*links*) de e-mails suspeitos. Escreva o endereço diretamente no *browser*;
7. Informações críticas ou dados pessoais só podem ser enviados em formato encriptado. As *passwords* devem ser enviadas por outro meio de comunicação.

NetEtiqueta

1. Evite escrever mensagens em MAIÚSCULAS com cores e a *bold*;
2. Tente ser claro e objetivo, produza textos simples com cuidado gramatical e ortográfico;
3. Tente ser educado e simpático, agradeça e cumprimente;
4. Pode usar *smileys* :-)) é uma forma simples de dar a entender os seus sentimentos;
5. Não reaja de forma emotiva porque normalmente escrevemos e-mails ou partilhamos o que não queremos;
6. Antes de publicar alguma informação verifique 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.

6 *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 confidenciais. 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 seu dinheiro ou os seus dados?”

Para recuperarmos os dados é necessário pagar um resgate.

Normalmente este ataque ocorre em 6 passos:

1. O *ransomware* entra via e-mail 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 seu PC;
5. O *software* começa a encriptar os seus dados;
6. Terminada a encriptação o *software* malicioso coloca uma mensagem no *desktop* com instruções para pagar o resgate com *Bitcoin*.

NOTA: Se o seu computador detetar um vírus ou suspeitar de um comportamento anormal por favor siga os **seguintes passos:**

1. Desligue o *Wi-Fi*;
2. Remova o cabo de rede (ou retire o portátil da *docking station*);
3. Não desligue o equipamento;
4. Contacte imediatamente a equipa TIC.



7 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.

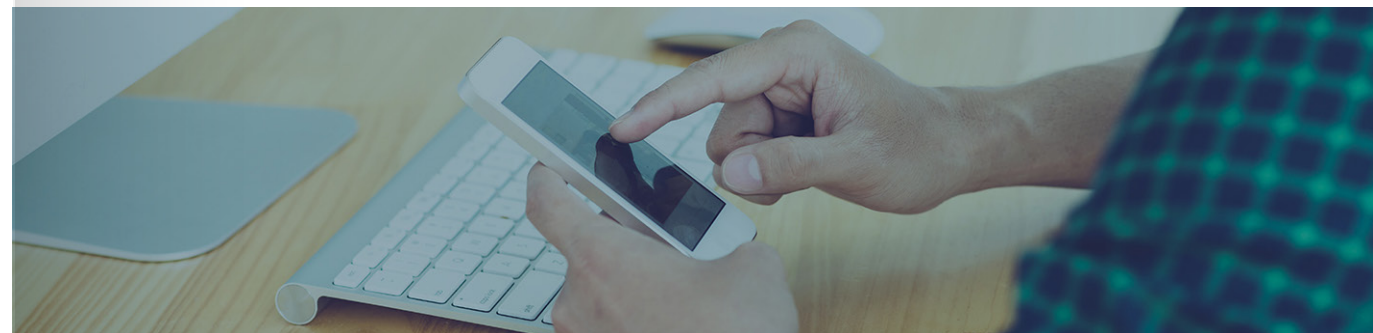
No mundo da internet existem regras e códigos de conduta com o objetivo de melhorar a segurança da informação.

Internet

- ✓ Certifique-se que o site é seguro fazendo duplo clique sobre o cadeado ou aceda pelo endereço (URL) que deve começar por “https://” e não por “http://”;
- ✓ Certifique-se que o seu *browser* e o antivírus estão atualizados e utilize uma *firewall* pessoal;
- ✓ Consulte os extratos das suas contas bancárias e de serviços com regularidade. Se encontrar algum movimento estranho, contacte imediatamente o prestador de serviço ou banco;
- ✓ Não é permitido aceder a sites com conteúdos ilegais ou inadequados;
- ✓ Atualize as suas *passwords*/PIN a cada 90 dias. Sempre que possível utilize *passwords* diferentes para sites seguros e sites não seguros;
- ✓ Não é permitido utilizar serviços públicos de e-mail, de transferência de ficheiros e ou serviços *cloud* para troca de dados da organização;
- ✓ Não é permitido divulgar informação ou dados nas redes sociais;
- ✓ Não é permitido jogar ou fazer apostas online com recursos da nossa organização (REDE, PCs, etc.).

Comunicação

- ✓ Quando fala ao telefone tenha cuidado para não divulgar informação confidencial;
- ✓ Evite falar de assuntos de trabalho em locais e transportes públicos, proteja-se contra os ouvintes;
- ✓ Evite ler informações críticas ou confidenciais em locais e transportes públicos;
- ✓ Evite abrir envelopes com dados confidenciais em espaços públicos;
- ✓ Não utilize redes sociais ou ferramentas (APPs) públicas para comunicar com parceiros e fornecedores (ex: WhatsApp ou Wunderlist), estas não são seguras;
- ✓ Não divulgue a extensão telefónica, e-mail e telemóvel de um colega sem que este o permita;
- ✓ Não coloque informações da organização em sites públicos (ex. Dropbox);
- ✓ Não registe o seu endereço de e-mail de trabalho em redes sociais;
- ✓ Não é permitido enviar dados da organização para e-mails pessoais (Ex. Gmail, Hotmail, etc.);
- ✓ Pense nas consequências antes de publicar qualquer informação, uma informação embaraçosa pode comprometer a sua imagem e a da sua organização.





8

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.

Olhe para os seus dispositivos móveis (telemóvel, portátil, PEN, token, pasta de documentos) e verifique 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 ligue o seu 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.

9 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 organização informa todos as entidades envolvidas;
- ✓ Todos os privilégios são imediatamente eliminados;
- ✓ Todos os equipamentos são desligados e recolhidos.

10 GDPR

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 transitório 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 na língua portuguesa se designa por Encarregado de Proteção de Dados;

É importante saber:

- ✓ O que são dados pessoais - são todas as informações relativas a uma pessoa **identificada** ou **identificável** (nome, morada, património, vencimento, datas, números de cartões, n.º de telefone, IP, vídeos, imagem, raça, dados biométricos, folhas de presença, avaliações, *curriculum vitae*, etc);
- ✓ Não deve reunir dados pessoais em papel ou em formato eletrónico sem informar o DPO;
- ✓ Cuidado ao enviar dados pessoais, estes devem estar sempre encriptados ou protegidos;
- ✓ Cuidado ao destruir ou eliminar dados pessoais, estes devem ser definitivamente apagados ou eliminados de forma a não serem recuperados por terceiros;
- ✓ Cuidado com os dados pessoais que troca com os seus parceiros e em especial com parceiros fora da EU;
- ✓ Documentos com dados médicos, e dados de menores são muitos sensíveis pelo que deve ter um cuidado redobrado na sua utilização;
- ✓ Se perder ou lhe roubarem dados pessoais informe de imediato o seu 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. No processo de destruição a empresa produz um relatório detalhado com a descrição dos dispositivos, quantidade e código de barras.
2. A documentação e certificados de destruição ficarão à guarda do CISO.
3. A destruição de grandes volumes de papel é feita a pedido.
4. 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.
5. 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.
6. Os equipamentos eletrónicos *media* só podem ser destruídos ou ter os dados apagados pelas TIC.

12 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 identificar um teclado diferente mais elevado ou com a ranhura de leitura de cartões alterada, escolha outro ATM;
2. Compre 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. Utilize apenas cartões de crédito pré-pagos e carregados com o valor necessário para a compra;
5. Evite fazer compras em *websites* fora da União Europeia, pois poderá 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 seus cartões.

Sempre que possível utilize o **contactless**, é a melhor forma de proteger o seu 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 seu PIN. Isto é, quanto menos vezes utilizar o seu código PIN mais protegido está o seu dinheiro.

Proteja o seu código PIN!!!

13 Dez Mandamentos de Segurança

1. Não introduzirás *PENs* alheias no PC de trabalho.
2. Não deixarás o teu PC desbloqueado, mesmo entre amigos ou colegas.
3. Não esquecerás os *backups* e apostarás nas redundâncias.
4. Não esquecerás o antivírus.
5. Não cobiçarás *phishing* alheio.
6. Assumirás o papel de melhor linha de defesa contra os ciberataques.
7. Não desejarás trabalhar fora de ambientes de redes seguras.
8. Não partilharás *passwords* e códigos de acesso.
9. Amarás as medidas de segurança sobre todas as coisas.
10. Não procrastinarás as atualizações, mesmo aos domingos e feriados.



A SEGURANÇA DA INFORMAÇÃO DA NOSSA
ORGANIZAÇÃO TAMBÉM **DEPENDE DE SI!**