CESPU

CESCE SI

# DISPOSITIVOS MÓVEIS E TELETRABALHO

## RISCOS E PROTEÇÃO

GABINETE DE **GESTÃO DA QUALIDADE E AUDITORIAS**
— PROTEÇÃO DE DADOS

GABINETE DE **GESTÃO DA QUALIDADE E AUDITORIAS**
— PROTEÇÃO DE DADOS
COORDENAÇÃO **BRIGITE SILVA**
ENCARREGADO DE PROTEÇÃO DE DADOS **(DPO)**

CONTACTOS
**11105** (EXTENSÃO)
BRIGITE.SILVA@**CESPU**.PT
PROTECAO.DADOS@CESPU.PT

FONTE:
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

# 01. DISPOSITIVOS MÓVEIS E O TELETRABALHO

## TRABALHO A PARTIR DE QUALQUER LUGAR

Consultar o email, aceder ou modificar um documento importante, são algumas das tarefas que podem ser feitas a partir de um dispositivo móvel.

## ESSENCIAL PARA O TRABALHO

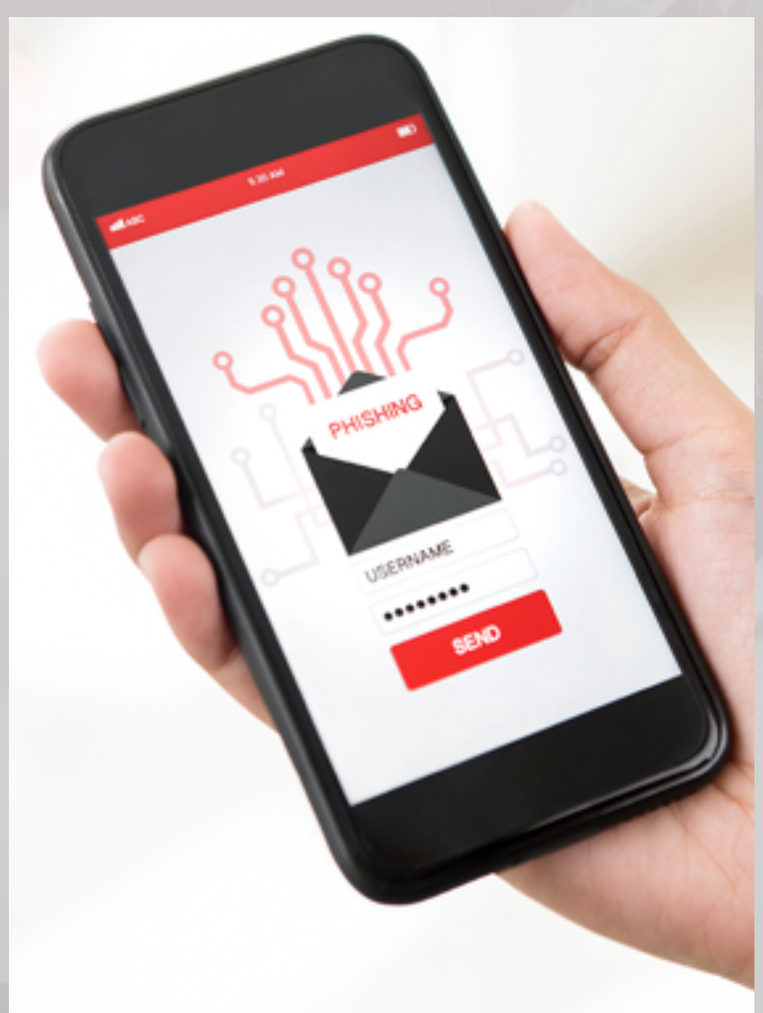
Hoje em dia, estes dispositivos tornaram-se ferramentas essenciais para o trabalho, graças à sua mobilidade e à facilidade de ligação à Internet.

## NOVOS RISCOS PARA A EMPRESA

Todas as novas possibilidades oferecidas pelos dispositivos móveis, para trabalhar, tornaram-se também novos riscos para a empresa que os próprios trabalhadores devem ter em conta.

FONTE:
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

# 02. RISCOS ASSOCIADOS




Os dispositivos móveis, os tablets e os computadores portáteis, devido à sua pequena dimensão e às suas capacidades para tratar de informação corporativa, representam novos riscos. No teletrabalho, utilizamos dispositivos móveis, ligamo-nos de fora da rede da empresa, utilizamos serviços para partilhar documentos e contamos com os riscos associados a um ambiente de trabalho não tão controlado.

## ROUBO OU PERDA

O **roubo ou perda** de telemóveis, tablets, computadores portáteis e dispositivos de armazenamento, tais como discos rígidos externos e pendrives.
Este pode ser o risco mais importante a que estes dispositivos estão expostos devido ao seu tamanho e, em muitos casos, ao seu elevado custo.

## INFEÇÃO POR MALWARE

A **infeção por malware** é sempre um risco a ter em conta, uma vez que o malware pode roubar informações confidenciais e as credenciais de acesso aos diferentes recursos. Muitas vezes negligenciamos a proteção contra malware nos equipamentos móveis.

FONTE:
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

# 02. RISCOS ASSOCIADOS


## SITES WEB FRAUDULENTOS

**Sites web fraudulentos**, a publicidade agressiva ou as páginas web do tipo phishing são as principais ameaças a que estão expostos. Navegar a partir dos dispositivos pequenos , particularmente telemóveis, é arriscado porque é mais difícil "livrar-se" desta publicidade.

## REDES WIRELESS INSEGURAS

A utilização de **redes wireless inseguras** pode colocar em risco a privacidade das comunicações, uma vez que os cibercriminosos podem estar a ”escutar" tudo o que é enviado e recebido. Por vezes podemos estar a ligar a redes wireless que imitam as redes wireless legítimas.

FONTE:
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

# 02. RISCOS ASSOCIADOS

## APLICAÇÕES

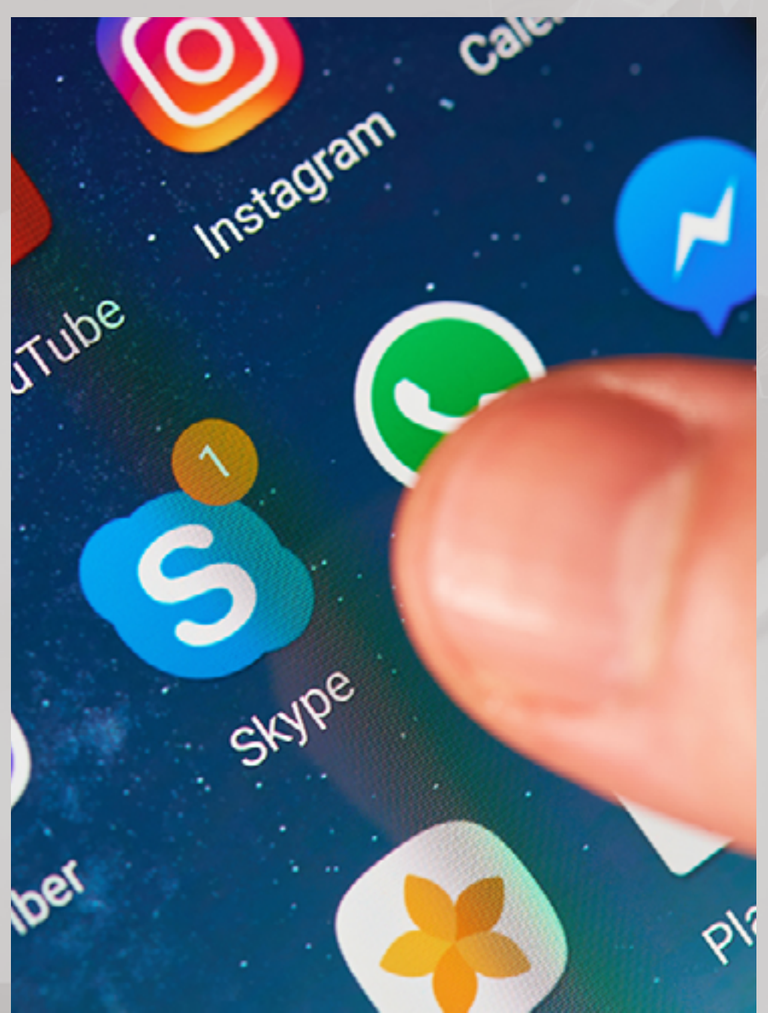
Instalação de aplicações que necessitam de acesso a determinadas permissões dos dispositivos, por vezes excessivas ou desnecessárias (tais como o acesso à câmara, contactos ou ficheiros), para poderem funcionar normalmente, podem comprometer a privacidade da informação corporativa.

## DISPOSITIVOS QUE NÃO CONTAM COM CONTROLOS DE ACESSO ROBUSTOS QUE OS PROTEJAM DE UM DESCUIDO, ROUBO OU PERDA.

A ausência destes ou a utilização de alguns considerados fracos, tais como o bloqueio standard do ecrã, constituem um risco de segurança.

FONTE:
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

# 02. RISCOS ASSOCIADOS




## ATUALIZAÇÕES

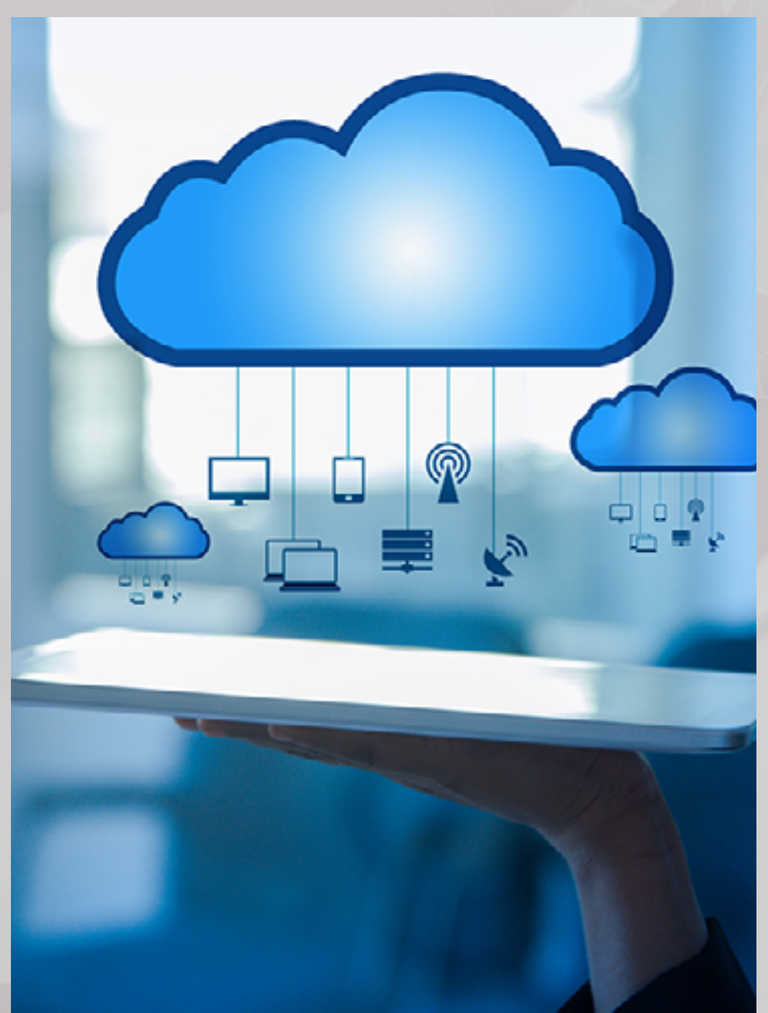
Tanto o sistema operativo, como as aplicações desatualizadas representam um risco para a segurança de toda a informação que gerem.

## MODIFICAÇÕES

A modificação dos controlos de segurança impostos pelos fabricantes. Alguns utilizadores decidem alterar as configurações dos seus dispositivos (jailbreak), o que pode constituir um risco grave, uma vez que os controlos de segurança impostos pelo fabricante são removidos.

FONTE:
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

# 02. RISCOS ASSOCIADOS



## ARMAZENAMENTO DA PASSWORD

Permitir que o dispositivo ou a aplicação armazenem as credenciais de acesso. Se um terceiro aceder ao dispositivo, terá acesso a todos os serviços onde a palavra-passe é armazenada.

## CLOUD

A utilização de serviços na cloud pode representar um risco, uma vez que a informação da empresa estará armazenada num terceiro.
Existe o risco de, se não for possível ligar à Internet (problemas de rede, tais como congestionamento ou inatividade), a informação armazenada na nuvem não estar acessível.

FONTE:
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

# 03. MEDIDAS DE PROTEÇÃO
## — PROTEÇÃO ANTIMALWARE E SITES WEB PERIGOSOS


O perigo de infeção causada por qualquer tipo de malware, está sempre presente. Todos os tipos de código malicioso podem chegar por e-mail e mensagens, em pendrives, através do browser ou através de aplicações

### FORMAÇÃO
Formação dos colaboradores para que sejam capazes de detetar ligações e ficheiros suspeitos, navegar de forma segura e descarregar aplicações confiáveis.

### FERRAMENTAS ANTIMALWARE E ANTIVIRUS
**Dispor de ferramentas que detetem e eliminem os vírus. Os sistemas antivírus deverão estar sempre atualizados** com a última versão, o que permitirá identificar dos vírus mais recentes. Por vezes, os antivírus também contam com ferramentas que permitem identificar possíveis sites web fraudulentos e perigosos, como aqueles que são utilizados para cometer ataques do tipo phishing. Ao selecionar um antivírus para o seu telemóvel, deverá verificar se este possui estas características.

FONTE:
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

# 03. MEDIDAS DE PROTEÇÃO
## — PROTEÇÃO CONTRA ACESSOS NÃO AUTORIZADOS


**Proteção contra acessos não autorizados:** Para evitar que terceiros sem permissão acedam a toda a informação é necessário que se implementem um conjunto de controlos:

· **Log-in**

**Passwords de aplicações,** se o dispositivo o permitir, especialmente em computadores portáteis. Desta forma evita-se que os outros utilizadores utilizem o dispositivo.

· **Contas de utilizadores e permissões**

Nos sistemas operativos como Windows, MacOS ou baseados em Linux,  é permitida a criação de diferentes utilizadores, e atribuir uma série de privilégios de acordo com o perfil do utilizador. É recomendável que cada utilizador conte com os privilégios mínimos e necessários que permitam desempenhar as suas funções. Deverão também utilizar password fortes.

· **Bloqueio do dispositivo**

Nos dispositivos baseados no Android ou iOS devem estabelecer o bloqueio de ecrã para o tempo mais curto possível e uma palavra-passe de desbloqueio forte. Também podem utilizar métodos biométricos para desbloquear os equipamentos.

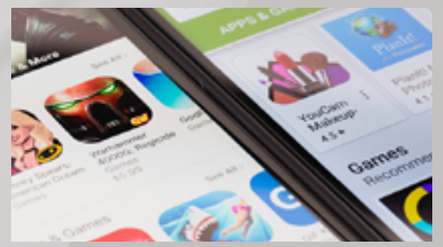
FONTE:
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

# 03. MEDIDAS DE PROTEÇÃO
## — PROTEÇÃO DA INFORMAÇÃO

· Encriptação da informação confidencial

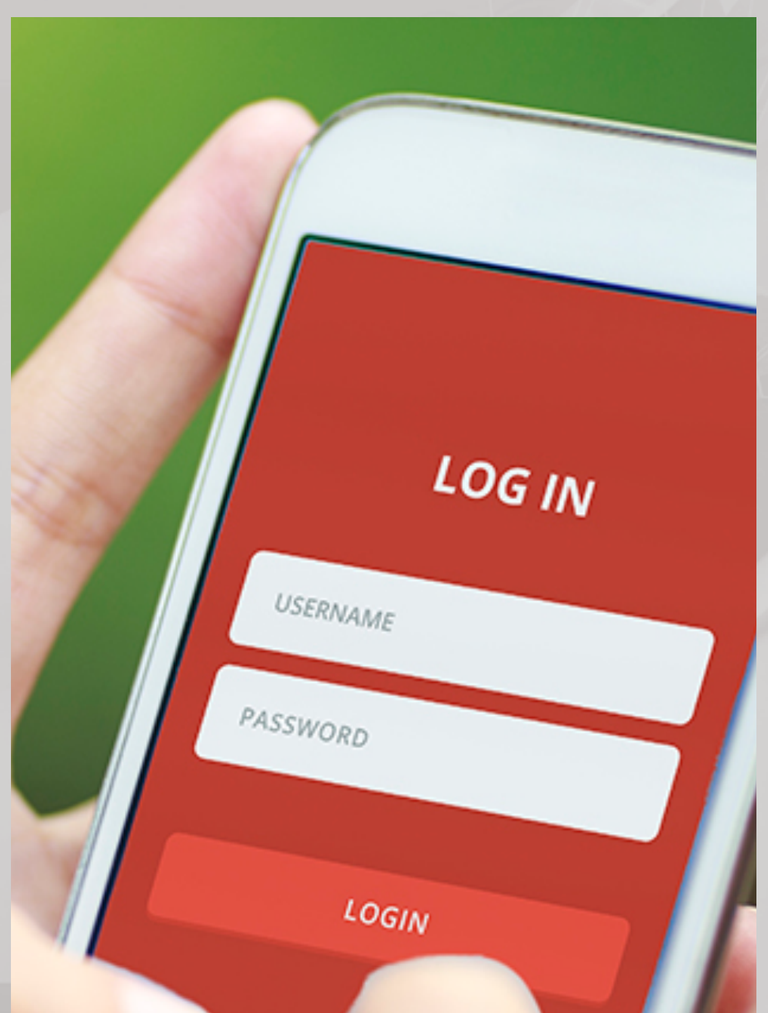
# 03. MEDIDAS DE PROTEÇÃO
## — APLICAÇÕES LEGÍTIMAS

· Encriptação da informação confidencial
· Lojas oficiais exclusivamente
· Downloads de origens legítimas e software atualizado



FONTE:
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

# 03. MEDIDAS DE PROTEÇÃO
## — NÃO ARMAZENAR AS PASSWORDS




· **«Lembrar palavra-passe»** não deve usar-se em dispositivos móveis.

A função **"lembrar a password"** nunca deve ser utilizada em dispositivos móveis, pois o acesso não autorizado poderia resultar no acesso a todos os serviços onde esta função tenha sido ativada. Em caso de utilizar múltiplos serviços, com diferentes palavras-passe, é recomendável utilizar um gestor de passwords que ajude nessa tarefa.

Exemplo de um gestor de password: **Keepass**

FONTE:
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

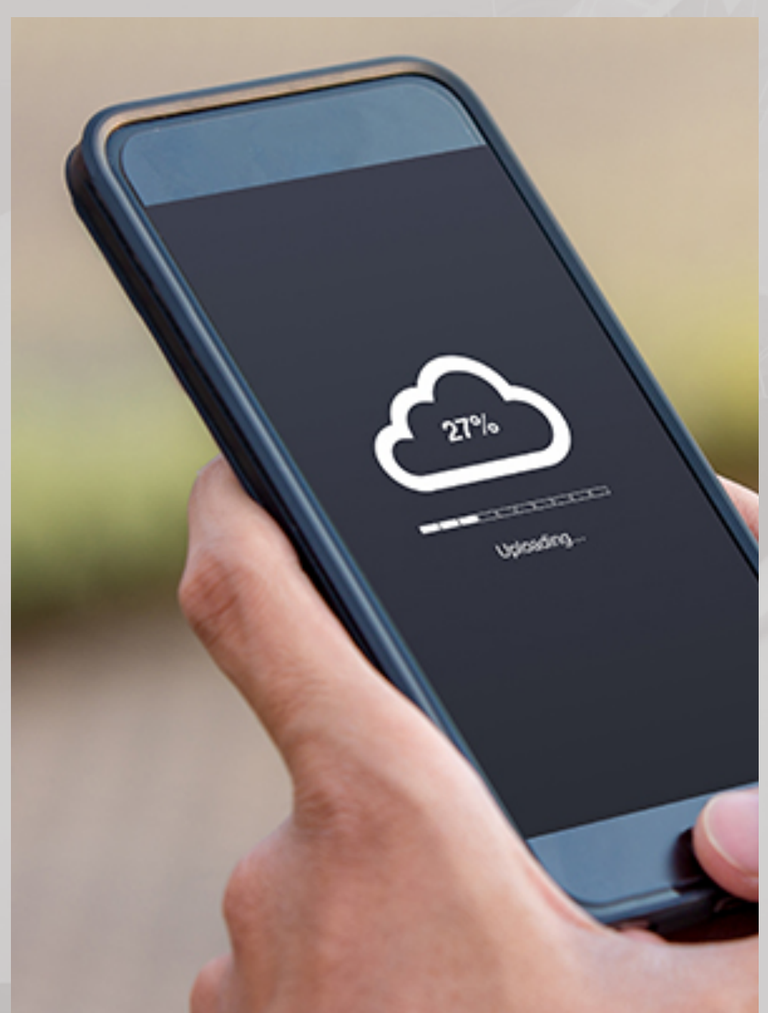

# 03. MEDIDAS DE PROTEÇÃO
## — NÃO UTILIZAR REDES WIRELESS INSEGURAS

· **Redes wireless públicas:** Com frequência nos encontramos em diferentes estabelecimentos e serviços públicos que oferecem conexão wireless de forma gratuita. **Não é recomendável utilizar estas conexões wireless** que encontramos nos hóteis, restaurantes, estações de comboio, aeroportos, etc., com dispositivos empresariais, uma vez que não conhecemos a sua segurança, nem a sua legitimidade e a privacidade da informação que enviamos ou recebemos poderá ser comprometida.

· **Utilizar rede móvel: É sempre a melhor opção utilizar a conectividade móvel 4G** que incorporam nos dispositivos (ligação de dados), especialmente quando se realizam tarefas sensíveis como o acesso ao banco online ou informação confidencial.

· **Rede Privada Virtual ou VPN:** Se é habitual viajar por motivos de trabalho e necessita de dispor de acesso à empresa, deve utilizar uma VPN (rede privada virtual) que encripte as ligações ponta a ponta, para aceder aos recursos da empresa. Deverá evitar, na medida do possível, utilizar aplicações de escritório remoto para  se ligar aos servidores da empresa sem VPN.

FONTE:
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD




# 03. MEDIDAS DE PROTEÇÃO
## — OUTRAS MEDIDAS DE PROTEÇÃO PARA O TELETRABALHO

· **Uso exclusivo para trabalhar:** Não permitir a utilização dos equipamentos da empresa por parte de outros utilizadores para jogos, downloads, etc.

· **Cópias de segurança:** realizar cópias de segurança de forma periódica.

· **Proteção da rede wireless doméstica:** No caso de utilizar uma rede wireless doméstica, seguir as seguintes recomendações e evitar acessos não autorizados:

- **WPA2 ou WPA3**
- **Chave de acesso robustas**
- **Desativar WPS**

VOLTAR AO INÍCIO

FONTE:
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD