Recomendações de Segurança e Proteção de Dados Privados

1 Informação encriptada em computadores pessoais (portáteis ou *desktops*)

De acordo com as orientações aos investigadores sobre proteção de dados em investigação científica (ver ponto E1.d das Orientações), a encriptação de dados pessoais que tenham o Iscte como responsável pelo tratamento é obrigatória em computadores pessoais. Recomenda-se a utilização de algum tipo de proteção integral dos dispositivos, recorrendo a técnicas de encriptação total do suporte de informação (disco, sistema de ficheiros). No caso de computadores Windows (Windows 10, por exemplo), recorrendo ao Bitlocker e, no caso do MacOS, recorrendo ao FileVault. Abaixo providencia-se alguma informação adicional para cada um dos sistemas operativos.

Windows (utilização do Bitlocker):

- https://carbidesecure.com/resources/how-to-encrypt-a-hard-drive-with-bitlocker-in-windows-10/
- https://www.windowscentral.com/how-use-bitlocker-encryption-windows-10

MacOS (utilização do FileVault):

- https://support.apple.com/en-us/HT204837
- https://support.apple.com/en-gb/guide/deployment/dep82064ec40/web
- https://www.computerworld.com/article/3643332/how-to-use-filevault-to-protect-business-data-on-macs.html

Por outro lado, podemos igualmente usar ferramentas que permitem a encriptação de alguns dados (ficheiros, pastas, etc.) recorrendo a ferramentas mais comuns, como o 7-Zip (https://www.7-zip.org) ou até mesmo o Winzip (https://www.winzip.com). Ambas são ferramentas para Windows e suportam a criação de ficheiros comprimidos com suporte para diversos tipos de encriptação. Para utilizadores MacOS, ferramentas como o BetterZip (https://betterzip.com).

2 Informação encriptada em dispositivos amovíveis

É igualmente obrigatória a utilização de algum tipo de tecnologia de encriptação em dispositivos amovíveis, como por exemplo discos externos ou *pens* USB. Abaixo indicam-se algumas soluções para diversos tipos de sistemas operativos.

Windows:

- Utilização do Bitlocker
  - https://www.dummies.com/article/technology/computers/operating-systems/windows/windows-10/how-to-use-bitlocker-for-encryption-on-removable-drives-140229
  - https://www.uvm.edu/it/kb/article/encrypt-external-drive/

MacOS:

- Utilização do FileVault

- https://www.uvm.edu/it/kb/article/encrypt-external-drive/
- https://support.apple.com/en-gb/guide/disk-utility/dskutl35612/mac

Existem ainda um conjunto de ferramentas de encriptação, que podem ser recomendadas e que funcionam em múltiplas plataformas.

- VeraCrypt (Windows, MacOS): https://www.veracrypt.fr/en/Home.html
- AxCrypt (Windows, MacOS): https://www.axcrypt.net/
- CipherShed (Windows, MacOS): https://www.ciphershed.org/
- DiskCryptor (Windows): https://diskcryptor.org/
- Cryptomator (Windows, MacOS): https://cryptomator.org/
- AESCrypt (Windows, MacOS): https://www.aescrypt.com/

Algumas das ferramentas, acima listadas, suportam igualmente sistemas operativos móveis como o Android e o iOS, o que significa que podem funcionar igualmente em *smartphones* ou *tablets*.

De igual forma, podem ser usadas aqui igualmente as ferramentas citadas anteriormente, como o 7-Zip, Winzip ou BetterZip (conforme a plataforma de escolha).

3 Transmissão de dados privados através da WWW – HTTPS e VPN

Deve ser sempre observada a segurança da ligação entre o navegador e o servidor de web, assegurando-se que está a ser utilizada uma ligação HTTPS (por oposição a HTTP). Isto é facilmente observável no navegador web, quer através da própria URL, quer através da visualização das propriedades da ligação no navegador.

Outra recomendação prende-se com a utilização de uma VPN, particularmente quanto estiver em causa a utilização de redes sem fios (Wi-Fi), em locais não-confiáveis. Recomenda-se a utilização da VPN do Iscte, mas se tal não for possível, deve ser usado qualquer outro fornecedor de VPN. O seguinte endereço oferece uma listagem de fornecedores de VPN, que pode ser usado para fazer uma comparação entre os mesmos (a maior parte destes serviços são comerciais, mas alguns deles oferecem a possibilidade de acesso gratuito limitado):

- Lista de VPNs: https://www.vpnranks.com/vpn-comparison/
- Comparação de VPNs: https://www.topvpncomparison.com/

4 Armazenamento seguro na nuvem *(cloud)*

Não se recomenda o uso de serviços de nuvem *(cloud)* externos à organização. Contudo, se por alguma razão imperativa não for possível usar os serviços institucionais, é importante selecionar serviços que encriptem os dados na nuvem. Deve sempre evitar-se colocar dados não-encriptados em serviços de nuvem; em alternativa, os ficheiros devem ser cifrados localmente nos computadores antes de serem armazenados em serviços de nuvem.

De seguida apresentam-se um conjunto de serviços de armazenamento seguro na nuvem que podem ser usados, em alternativa aos serviços de nuvem da organização:

- Sync: https://www.sync.com/
- pCloud: https://www.pcloud.com/
- IceDrive: https://icedrive.net/
- Mega: https://mega.io/
- iDrive: https://www.idrive.com/
- Tresorit: https://tresorit.com/
- BoxCryptor: https://www.boxcryptor.com/en/

- NordLocker: https://nordlocker.com/
- Cryptomator: https://cryptomator.org/
- Nextcloud: https://nextcloud.com/
- ProtonDrive: https://drive.protonmail.com
- SpiderOak: https://spideroak.com/
- Egnyte: https://www.egnyte.com/

Alguns destes serviços são comerciais, enquanto outros são de utilização gratuita.

5 Envio de informação privada por correio eletrónico

Relativamente ao envio de dados privados através do correio eletrónico é igualmente importante observar requisitos relacionados com a encriptação dos mesmos. Aqui é importante distinguir entre os serviços de *webmail* e os clientes de email que são instalados nos nossos equipamentos terminais.

5.1 Serviços de Webmail

Os mais populares serviços de *webmail*, como o Gmail.com ou Outlook.com não oferecem aos utilizadores a possibilidade de poderem cifrar os emails que enviam de forma a que os mesmos apenas possam ser lidos pelos respetivos destinatários. Existem alguns serviços de *webmail online*, que oferecem este tipo de funcionalidade. A seguinte listagem indica alguns:

- ProtonMail: https://protonmail.com/
- Tutanota: https://tutanota.com/
- Mailfence: https://mailfence.com/

5.2 Clientes de Email

Os clientes de email que usamos nos nossos computadores e nos nossos dispositivos móveis possuem a possibilidade de encriptar os emails, através de alguns mecanismos que exigem algum tipo de configuração adicional dos mesmos. Os principais mecanismos são o S/MIME e o PGP (ou GPG).

5.2.1 S/MIME

S/MIME significa *Secure/Multipurpose Internet Mail Extensions* e é um protocolo utilizado para assinar e/ou encriptar digitalmente e-mails. Está implementado nos principais clientes de email, como o Microsoft Outlook, Apple Mail, Mozilla Thunderbird e muitos outros.

Alguns links úteis com informação adicional:

- O que é e como funciona o S/MIME?: https://kb.ptisp.com/o-que-e-como-funciona-o-s-mime/
- Instalando um S/MIME Certificado e envio de email seguro com o Outlook no Windows 10: https://www.ssl.com/pt/como/instalando-o-certificado-mime%2C-enviando-e-mail-seguro%2C-Outlook-Windows-10/
- Como instalar um certificado S/MIME no Outlook no Windows 11/10: https://geekingup.org/pt-br/como-instalar-um-certificado-s-mime-no-outlook-no-windows-11-10
- Installing the S/MIME Certificate on your Mac: https://itsecurity.uiowa.edu/resources/macClientCert
- Obtaining and using an S/MIME certificate on Apple MacOS: https://www.sslmarket.co.uk/ssl/obtaining-and-using-an-s-mime-certificate-on-apple-macos/
- MacOS: Using Email Encryption in Apple's Mail: https://www.macobserver.com/tips/quick-tip/macos-using-email-encryption-apples-mail/

5.2.2 PGP (ou GPG)

O PGP – Pretty Good Privacy (https://www.openpgp.org/) ou o GPG – GNU Privacy Guard (https://gnupg.org/) são dois outros exemplos de tecnologias que permitem efetuar a encriptação de correio eletrónico. Existem

múltiplas extensões de PGP ou GPG que podem ser usadas nos principais clientes de email, para permitir a encriptação de correio eletrónico.

Na seguinte ligação é possível ver a lista de clientes e de extensões, em diversos sistemas operativos (Windows, MacOS) que suportam o PGP:

- https://www.openpgp.org/software/