Interreg
España - Portugal

Cofinanciado por la Unión Europea
Cofinanciado pela União Europeia

CIBERIA

Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura

Guía de Buenas Prácticas dirigida a organismos de administración pública local y PYMEs

Actividad 3, Acción 3.1

Versión: 0.1
Nivel de difusión: Privado
Autores: JRaquel Abreu, Bernardo Sequeiros, Pedro Inácio

Historia del documento:

Acrónimo del proyecto	CIBERIA
Título del proyecto	Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura
Coordinador	Javier Prieto Universidad de Salamanca (USAL)
Duración	
Entregable	
Actividad	
Acción	
Nivel de difusión	Privado
Fecha de entrega	
Beneficiario responsable	
Beneficiarios participantes	

Fecha	Versión	Autor	Comentario

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

Acrónimos

2FA	Two Factor Authentication
ABAC	Attribute-Based Access Control
AD	Active Directory
AI	Artificial Intelligence
BCP	Business Continuity Plan
CNCS	Centro Nacional de Cibersegurança
CNPD	Comissão Nacional de Proteção de Dados
DAC	Discretionary Access Control
DRP	Disaster Recovery Plan
EDR	Endpoint Detection System
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IGMP	Internet Group Message Protocol
INCIBE	Instituto Nacional de Cibersegurança
IP	Internet Protocol
IPS	Intrusion Prevention System
IRP	Incident Response Plan
ISO	International Standards Organization
IT	Information Technologies
LLC	Logical Link Control
MAC	Mandatory Access Control
MeAC	Medium Access Control
MFA	Multi-Factor Authentication
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
RBAC	Role-Based Access Control
RGPD	Regulamento Geral sobre a Proteção de Dados
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

TLS	Transport Layer Security
UDP	User Datagram Protocol
UE	União Europeia
VPN	Virtual Private Network
WWW	World Wide Web

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

Índice

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

1. Introdução

Num mundo cada vez mais digital, a cibersegurança tornou-se um aspeto crucial da vida quotidiana. Dos dispositivos pessoais às redes empresariais, é essencial proteger os dados e os sistemas contra o acesso não autorizado, as ciberameaças e os ataques maliciosos. A cibersegurança não é apenas uma preocupação para os "informáticos". Todos têm um papel a cumprir para manter as suas informações seguras. Ao adotar boas práticas no que toca à cibersegurança, os riscos podem ser reduzidos significativamente.

Este guia tem como objetivo fornecer uma visão global de boas práticas de cibersegurança, que organizações e indivíduos podem seguir. Independentemente do grau de conhecimento na área da cibersegurança, este guia oferece conselhos práticos para melhorar a segurança e resiliência digitais.

As práticas aqui descritas foram concebidas para abordar diversos temas importantes da cibersegurança, desde a utilização de Palavras-passes Seguras, à Gestão do Correio Eletrónico, passando também por aspetos mais técnicos como a Monitorização de Redes e o Uso de Servidores.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

2. Conceitos

2.1. Introdução

Este capítulo tem como objetivo principal a explicação de conceitos técnicos de maior relevância para a interpretação deste guia. No entanto, estas explicações serão feitas de forma sucinta, apenas para que o leitor consiga entender os diferentes conceitos ao longo do documento.

2.2. Modelo OSI

O modelo de referência de rede *Open Systems Interconnection* (OSI) [1, 2] foi desenvolvido pela *International Standards Organization (ISO)* com o objetivo de primeiramente padronizar a maneira de se desenvolver uma solução para a troca de dados entre redes e dentro de uma própria rede.

Este modelo tenta padronizar a forma de transmitir dados na rede. Isto permite o desenvolvimento de sistemas compatíveis entre si, mesmo sendo de fabricantes diferentes. O termo *Open* no nome do modelo dá a entender a ideia de um sistema aberto à comunicação com outros sistemas.

O modelo OSI é baseado em **sete camadas**, sendo que cada camada resolve um problema específico relacionado com a transmissão de dados na rede.

A figura 1, apresentada de seguida, representa o modelo OSI.

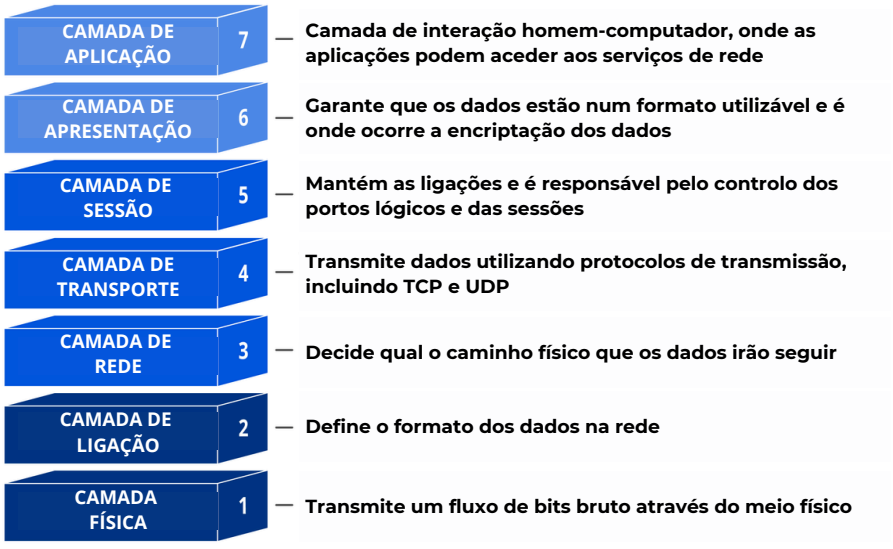

Figura 1: Modelo OSI, com uma explicação sucinta das camadas.(Imagem adaptada de [3])

- Camada Física - *Layer* 1

A camada física refere-se ao meio de comunicação físico e às tecnologias de transmissão de dados através desse meio. Essencialmente, a comunicação de dados é a transferência de sinais digitais e eletrónicos através de vários canais físicos, como cabos de fibra ótica, cabos de cobre e ar. A camada física inclui normas para tecnologias e métricas estritamente relacionadas com os canais, como Bluetooth, NFC e velocidades de transmissão de dados.

- Camada de Ligação (ou Enlace) de dados - *Layer* 2

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

A camada de ligação de dados é muito semelhante à camada de rede, exceto que a camada de ligação de dados facilita a transferência de dados entre dois dispositivos na mesma rede. A camada de ligação de dados recebe os pacotes da camada de rede e divide-os em partes mais pequenas, designadas por *frames*. Tal como a camada de rede, a camada de ligação de dados também é responsável pelo controlo do fluxo e do erro nas comunicações intra-rede (a camada de transporte apenas efetua o controlo do fluxo e de erros nas comunicações inter-rede).

Esta camada subdivide-se em duas subcamadas: a subcamada superior de controlo de acesso ao meio (*Logical Link Control (LLC)*) e a subcamada inferior de controlo das ligações lógicas (*Medium Access Control (MeAC)*).

- Camada de Rede - *Layer* 3

A camada de rede é responsável por facilitar a transferência de dados entre duas redes diferentes. Se os dois dispositivos que estão a comunicar estiverem na mesma rede, a camada de rede é desnecessária. A camada de rede divide os segmentos da camada de transporte em *Protocol Data Units (PDUs)* mais pequenas, designadas por pacotes, no dispositivo emissor, e volta a montar estes pacotes no dispositivo recetor. A camada de rede também encontra o melhor caminho físico para os dados chegarem ao seu destino, o que é conhecido como encaminhamento.

Os protocolos da camada de rede incluem o IP, o ICMP, o IGMP e a *suite* IPsec.

- Camada de Transporte - *Layer* 4

A camada 4 é responsável pela comunicação de ponta a ponta entre dois dispositivos. Isto inclui a recolha de dados da camada de sessão e a sua divisão em partes chamadas segmentos antes de os enviar para a camada 3 (camada de rede). É nesta camada que é realizada a segmentação de dados e sequenciação.

A camada de transporte é também responsável pelo controlo de fluxo e pelo controlo de erros. O controlo de fluxo determina uma velocidade de transmissão ótima para garantir que um remetente com uma ligação rápida não sobrecarregue um recetor com uma ligação lenta. A camada de transporte efetua o controlo de erros na extremidade recetora, assegurando que os dados recebidos estão completos e solicitando uma retransmissão se não estiverem.

Os protocolos da camada de transporte incluem o TCP e o UDP.

- Camada de Sessão - *Layer* 5

A camada de sessão é a camada responsável por abrir e fechar a comunicação entre dois dispositivos. O tempo entre a abertura e o fecho da comunicação é designado por sessão. A camada de sessão garante que a sessão permanece aberta o tempo suficiente para transferir todos os dados que estão a ser trocados e, em seguida, fecha imediatamente a sessão para evitar o desperdício de recursos. A camada de sessão também sincroniza a transferência de dados com os pontos de controlo.

- Camada de Apresentação - *Layer* 6

Esta camada é principalmente responsável pela preparação dos dados para que possam ser utilizados pela camada de aplicação; ou seja, a camada de apresentação torna os dados apresentáveis para serem consumidos pelas aplicações. Esta camada é responsável pela tradução, encriptação e compressão dos dados.

Esta camada também é responsável pela compressão dos dados que recebe da camada de aplicação antes de os entregar à camada de sessão (camada 5). Isto ajuda a melhorar a velocidade e eficiência da comunicação, minimizando a quantidade de dados que serão transferidos.

- Camada de Aplicação - *Layer* 7

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027
Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

Esta é a única camada que interage diretamente com os dados do utilizador.
As aplicações de *software*, como os navegadores Web e os clientes de correio eletrónico, dependem da camada de aplicação para iniciar as comunicações. Mas, deve ficar claro, que as aplicações de *software*-cliente não fazem parte da camada de aplicação.
A camada de aplicação é responsável pelos protocolos e pela manipulação de dados em que o *software* se baseia para apresentar dados significativos ao utilizador.

Os protocolos da camada de aplicação incluem o HTTP e o SMTP.

2.3. Protocolos de Rede

No que se refere às redes, um protocolo [4] é um conjunto de regras para a formatação e processamento de dados. Estes dispositivos são como uma linguagem comum para os computadores. Os computadores dentro de uma rede podem usar *software* e *hardware* muito diferentes, no entanto, o uso de protocolos permite que eles comuniquem uns com os outros independentemente dessas diferenças.

Na Internet, existem diferentes protocolos para diferentes tipos de processos. Já na secção acima foram referidos alguns protocolos que se encontram em diferentes camadas do modelo OSI.
Em baixo, encontram-se definições dos protocolos acima referidos. Estas definições são muito sucintas, visto que o foco deste documento não são os protocolos de rede.

Hypertext Transfer Protocol (HTTP)
Hypertext Transfer Protocol [5] (HTTP) é utilizado para carregar páginas na Internet através de hiperligações. O *Hypertext Transfer Protocol* [5] (HTTP) é um protocolo de comunicação (na camada de aplicação do modelo OSI utilizado para sistemas de informação de hipermédia distribuídos e colaborativos. Este protocolo é a base de comunicação para a *World Wide Web (WWW)*, onde os documentos de hipertexto incluem hiperligações para outros recursos a que o utilizador pode aceder facilmente. Resumindo, o protocolo HTTP é utilizado para carregar páginas na *Internet* através de hiperligações.

Simple Mail Transfer Protocol (SMTP)
O *Simple Mail Transfer Protocol* [6] (SMTP) é um protocolo de comunicação usado para enviar e receber mensagens de e-mail pela *Internet*. Servidores de e-mail e outros agentes de transferência de mensagens usam este protocolo para enviar, receber e retransmitir e-mails.

Internet Protocol (IP)
O *Internet Protocol* [7] (IP) é um conjunto de requisitos que permite que os dispositivos comuniquem entre si através da *Internet*. Cada dispositivo ligado à *Internet* tem um endereço IP único que ajuda os dados a saberem onde devem ir e de onde vêm. Este protocolo pode ser utilizado com vários protocolos de transporte, incluindo TCP e UDP.

Transmission Control Protocol (TCP)
O *Transmission Control Protocol* [8] (TCP) é um dos principais protocolos do conjunto TCP/IP. Situa-se entre as camadas de aplicação e de rede, que são utilizadas para fornecer serviços de entregas fidedignos. Este protocolo assegura uma transmissão de dados segura e eficiente através da *Internet*. TCP desempenha um papel essencial na gestão do fluxo de dados entre computadores, garantindo que a informação é entregue com precisão e na sequência correta.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027
Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

User Datagram Protocol (UDP)
O *User Datagram Protocol* [9] (UDP), um protocolo de comunicação da camada de transporte, é um protocolo muito comum para o tráfego de voz e vídeo. Ao contrário do protocolo TCP, este não tem ligação e não garante a entrega, a ordem, ou a verificação de erros, o que o torna uma opção leve e eficiente para determinados tipos de transmissão de dados.

Internet Control Message Protocol (ICMP)
O *Internet Control Message Protocol* [10] (ICMP) é um protocolo da camada de rede. Este é principalmente em equipamento de rede, como os *routers*, e é utilizado para o tratamento de erros na camada de rede. Uma vez que existem diversos tipos de falhas nesta camada, o ICMP pode ser utilizado para comunicar e resolver esses erros.

Internet Group Message Protocol (IGMP)
O *Internet Group Message Protocol* [11] (IGMP) é um protocolo que permite que vários dispositivos partilhem um endereço IP para que todos possam receber os mesmos dados. O IGMP é um protocolo da camada de rede utilizado para configurar a difusão múltipla em redes que utilizam o IP versão 4 (IPv4); especificamente, este protocolo permite que os dispositivos se juntem a um grupo de *multicasting*.

IPsec
O IPsec [12] é um grupo de protocolos para proteger as ligações entre dispositivos. Este protocolo ajuda a manter seguros os dados enviados através de redes públicas. É frequentemente utilizado para configurar Virtual Private Networks (VPNs) e funciona através da encriptação de pacotes IP, juntamnete com a autenticação da fonte de onde provêm os pacotes.

2.4. Outras definições importantes

Há outras definições que poderão ser importantes ao longo do guia e que não se enquadram nas secções anteriores.
Esta secção apresenta essas definições.

VPN
Uma *Virtual Private Network* (VPN) é uma ligação cifrada através da Internet de um dispositivo a uma rede. A ligação cifrada ajuda a garantir que os dados sensíveis são transmitidos em segurança, impede que as pessoas não autorizadas “espiem” o tráfego e permite que um utilizador possa trabalhar remotamente.

Secure Sockets Layer (SSL)
O *Secure Sockets Layer* (SSL) é um protocolo de segurança que proporciona privacidade, autenticação e integridade às comunicações na Internet.

Transport Layer Security (TLS)
O *Transport Layer Security* (TLS) é um protocolo de segurança que fornece privacidade e integridade de dados para comunicações na Internet. A implementação deste protocolo é uma prática padrão para a criação de aplicações Web seguras.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027
Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

3. Normas e Leis de Cibersegurança em Portugal e em Espanha

A crescente digitalização de serviços e o aumento das ameaças cibernéticas têm impulsionado governos em todo o mundo a desenvolver legislações específicas para proteger infraestruturas críticas, dados sensíveis e cidadãos. Tanto em Portugal como em Espanha, as legislações e normas que regem a cibersegurança evoluíram para lidar com essas ameaças, e visam proteger a integridade das infraestruturas digitais, garantir a privacidade dos dados e fortalecer a resiliência diante de incidentes cibernéticos.

Os dois países, como membros da União Europeia (UE), seguem diretrizes comuns estabelecidas pela legislação europeia, especialmente no que diz respeito ao **Regulamento Geral de Proteção de Dados** (RGPD) e à diretiva Europeia NIS (*Network and Information Systems*). No entanto, cada país também possui leis e normas específicas que refletem as suas particularidades legislativas e os desafios próprios enfrentados no domínio da cibersegurança.

Este capítulo examina as normas e leis da cibersegurança em Portugal e Espanha, abordando tanto as regulamentações nacionais quanto as obrigações decorrentes das diretivas europeias. A análise proporciona uma visão abrangente sobre cada país está preparado para enfrentar as ameaças cibernéticas, bem como as semelhanças e diferenças nas suas abordagens legislativas.

3.1. CNCS

O **Centro Nacional de Cibersegurança** (CNCS) atua como coordenador operacional e autoridade especialista em matéria de cibersegurança junto as entidades do Estado, operadores de Infraestruturas Críticas Nacionais, operadores de serviços essenciais e prestadores de serviço digitais, garantindo que o ciberespaço é utilizado como espaço de liberdade, segurança e justiça, para a proteção dos setores da sociedade que materializam a soberania nacional e o Estado de Direito Democrático.

O CNCS atua em vários domínios, como a gestão de incidentes no ciberespaço de interesse nacional, através do CERT.PT (*Computer Emergency Response Team*, ou em português, Equipa de Resposta a Incidentes Informáticos), a cooperação nacional, a normalização e a sensibilização e treino. Para o efeito, disponibiliza quadros de referência e instrumentos que ajudam as organizações a adquirir maturidade em cibersegurança, recomendações técnicas, fiscalização, cursos e ações de sensibilização, conteúdos de boas práticas e relatórios que analisam o estado da arte do país nestas matérias.

Para mais informação, clique aqui.

3.2. INCIBE

O **Instituto Nacional de Cibersegurança** (INCIBE) [13] trabalha para reforçar a confiança digital, aumentar a cibersegurança e a resiliência e contribuir para o mercado digital de uma forma que promova a utilização segura do ciberespaço em Espanha.

O INCIBE é um instituto que depende do Ministério da Transformação Digital e Função Pública através da Secretaria de Estado da Digitalização e Inteligência Artificial e consolidou-se como uma entidade de referência para o desenvolvimento da cibersegurança e da confiança digital para os cidadãos, redes académicas e de investigação, profissionais, empresas e, especialmente para setores estratégicos.

Com uma atividade baseada na investigação, na prestação de serviços e na articulação com os agentes com competências na matéria, o INCIBE contribui para a construção da cibersegurança a nível nacional e internacional.

As principais missões do INCIBE são as seguintes:

- Melhorar a cibersegurança e a confiança digital dos cidadãos, instituições públicas espanholas e empresas privadas em Espanha;

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

- Proteger e defender os cidadãos, instituições públicas espanholas e empresas privadas em Espanha;
- Fortalecer o setor espanhol da cibersegurança;
- Promover a R&D&I (*Research and Development and Innovation*) espanhola no domínio da cibersegurança;
- Identificar, gerar, atrair e desenvolver profissionais no setor da cibersegurança;

Para mais informação, clique aqui.

3.3. Lei n.º 46/2018

De acordo com o Diário da República, a Lei nº. 46/2018 de 13 de agosto [14, 15] estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

O Regime Jurídico da Segurança do Ciberespaço aplica-se às entidades da Administração Pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais, aos prestadores de serviços digitais, bem como a quaisquer outras entidades que utilizem redes e sistemas de informação, nomeadamente, no âmbito da notificação voluntária de incidentes.

Estabelece no respetivo Capítulo II a Estrutura Nacional de Segurança no Ciberespaço, do qual faz parte o Conselho Superior de Segurança do Ciberespaço como órgão específico de consulta do Primeiro-Ministro para os assuntos relativos à segurança do ciberespaço. Este capítulo consagra ainda o Centro Nacional de Cibersegurança como Autoridade Nacional de Cibersegurança e o CERT.PT como Equipa de Resposta a Incidentes de Segurança Informática Nacional.

O Capítulo III determina as entidades às quais o Regime Jurídico da Segurança do Ciberespaço se aplica tenham de adotar requisitos de segurança e de notificar o Centro Nacional de Cibersegurança dos incidentes com um impacto relevante na segurança das respetivas redes e dos sistemas de informação.

Por fim, o Capítulo IV consagra o regime de fiscalização e sanções e o Capítulo V consagra as disposições finais, com destaque para o regime de identificação de operadores de serviços essenciais e dos prestadores de serviços digitais.

3.4. Decreto-Lei n.º 65/2021

O Decreto-Lei n.º 65/2021 de 30 de julho [16] define o Regime Jurídico da Segurança do Ciberespaço em Portugal, elencando as obrigações das entidades abrangidas no âmbito da certificação da cibersegurança e transpondo para a lei nacional o Regulamento (EU) 2019/881 do Parlamento Europeu (17 de abril de 2019). Este Decreto-Lei regulamenta também a Lei n.º 46/2018, apresentada anteriormente.

Assim, todos os Organismos da Administração Pública, Operadores de Infraestruturas Críticas e de Serviços Essenciais e Prestadores de Serviços Digitais ficam obrigados a:

- Comunicar ao CNCS a identidade e contactos do responsável de segurança e do contacto permanente da sua organização;
- Desenvolver um plano de segurança da informação;
- Elaborar um inventário onde constem todos os ativos e comunicá-lo ao CNCS;
- Elaborar relatórios anuais de segurança da informação e apresentá-los ao CNCS;
- Realizar uma avaliação de riscos a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação;
- Reportar incidentes de segurança ao CNCS com a maior brevidade possível.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

3.5. Regulamento n.º 183/2022

O Regulamento n.º 183/2022 do Gabinete de Segurança configura uma instrução técnica relativa à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventários de ativos, relatório anual e notificação de incidentes.

3.6. Comissão Nacional de Proteção de Dados

A **Comissão Nacional de Proteção de Dados (CNPD)** é uma entidade administrativa independente, com personalidade jurídica de direito público e com poderes de autoridade, dotada de autonomia administrativa e financeira, que funciona junto da Assembleia da República.

A CNPD **controla** e **fiscaliza** o **cumprimento do Regulamento Geral sobre a Proteção de Dados** (descrita imediatamente abaixo) e de outras leis, bem como das demais disposições legais e regulamentares em matéria de proteção de dados pessoais, a fim de defender os direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos dos seus dados pessoais.

3.7. Regulamento Geral de Proteção de Dados

O **Regulamento Geral sobre a Proteção de Dados** (RGPD) [17, 18] é um Diploma Europeu (EU 2016/679) que determina as regras relativas à proteção, ao tratamento e à livre circulação dos dados pessoais das pessoas nos países da União Europeia.

O Regulamento Geral sobre a Proteção de Dados (RGPD) reforça os direitos existentes, prevê novos direitos e confere aos cidadãos um maior controlo sobre os seus dados pessoais. Inclui as medidas seguidamente apresentadas:

- **Acesso facilitado dos cidadãos aos seus próprios dados:** inclui a prestação de mais informações sobre a forma como os dados são tratados e a garantia de que essas informações são disponibilizadas de forma clara e compreensível;
- **Um novo direito à portabilidade dos dados:** facilita a transmissão de dados pessoais entre os prestadores de serviços;
- **A clarificação do direito ao apagamento dos dados:** sempre que uma pessoa deixe de permitir o tratamento dos seus dados e não haja razões legítimas para a sua conservação, os dados serão apagados;
- **O direito de saber quando os dados pessoais foram violados:** as empresas e organizações devem notificar a autoridade de controlo da proteção de dados competente e, em casos de violações graves em matéria de dados, também as pessoas afetadas.

O RGPD poderá aplicar-se quando:

- Uma entidade esteja estabelecida na União Europeia (UE) (aplica-se independentemente de o tratamento ocorrer na UE);
- Uma entidade não estabelecida na UE forneça bens ou serviços (mesmo a título gratuito) a pessoas na UE. A entidade seja uma agência governamental, empresa pública ou privada, pessoa singular ou organização sem fins lucrativos;
- Uma entidade não esteja estabelecida na UE, mas monitorize o comportamento de pessoas que se encontrem na UE, desde que tal comportamento se verifique na UE.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

Existem também **obrigações a cumprir** por parte das entidades:

1. Designar o Encarregado de Proteção de Dados;
2. Adotar Políticas de Privacidade e de Segurança da Informação;
3. Realizar a Avaliação de Impacto sobre Proteção de Dados;
4. Obter o consentimento dos titulares para finalidades de tratamento específicas;
5. Tratar os dados recolhidos para finalidades determinadas, explícitas e legítimas;
6. Efetuar registos de atividades de tratamento de dados;
7. Prestar informação aos titulares dos dados;
8. Garantir os direitos de acesso, retificação, apagamento e oposição;
9. Assegurar os direitos de limitação do tratamento e portabilidade dos dados;
10. Conservar os dados apenas pelo período necessário;
11. Implementar os princípios de *privacy by design* e o *privacy by default*;
12. Implementar boas práticas e medidas adequadas de segurança;
13. Celebrar contratos escritos com os subcontratantes;
14. Notificar violações de dados e de incidentes de segurança;
15. Pedir, nos casos aplicáveis, consulta prévia à CNPD para os tratamentos de dados;
16. Realizar auditorias de conformidade.

É de realçar ainda que são as entidades que têm de comprovar que estão a cumprir o regulamento, e não como ocorria anteriormente, onde era o regulador que tinha de provar o incumprimento.

3.8. ISO/IEC 27000

A ISO 27000 é um **conjunto de certificações** de segurança da informação e proteção de dados para as empresas e órgãos públicos. As certificações da família ISO 27000 foram desenvolvidas em parceira entre a ISO e a *International Electrotechnical Commission*, outra organização dedicada à padronização, daí o nome ISO/IEC 27000.

Estas servem como base para a criação de um Sistema de Gestão de Segurança da Informação (SGSI) em organizações de pequeno, médio e grande porte. O SGSI reúne políticas, procedimentos, diretrizes e recursos de proteção de informação de uma organização. O sistema deve estar alinhado com os objetivos de negócio e ser gerido de forma conjunta pela empresa.

3.9. Diretiva SRI 2 (NIS 2)

A Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 [19] - atualmente em processo de transposição - relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a sua antecessora, a Diretiva (UE) 2016/1148 (Diretiva SRI 1).

Neste âmbito, a Diretiva SRI 2 visa atingir os mesmos três objetivos que a sua antecessora, em especial:

- Exigir que os Estados-Membros garantam um elevado nível de cibersegurança;

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

- Reforçar a cooperação europeia entre as autoridades competentes pela cibersegurança;
- Exigir que os principais operadores dos setores-chave da nossa sociedade adotem as medidas de segurança necessárias e notifiquem às autoridades competentes qualquer incidente que tenha impacto significativo na prestação dos seus serviços.

A Diretiva SRI 2 tem ainda como objetivo central eliminar as divergências profundas verificadas no contexto da aplicação da Diretiva SRI 1 entre os Estados-Membros, ambicionando uma maior harmonização através do estabelecimento de regras mínimas relativas ao funcionamento de um quadro regulamentar coordenado, entre outras medidas.

As principais diferenças da Diretiva SRI 2 face à Diretiva SRI 1 resumem-se da seguinte forma:

- O âmbito de aplicação da NIS 2 foi amplamente alargado - foram adicionados novos setores e novos tipos de entidades dentro dos setores existentes;
- A estruturação dos setores abrangidos foi alterada - existem dois grupos de setores, os Setores de Importância Crítica e os outros setores críticos;
- A categorização das entidades abrangidas foi alterada - nesta Diretiva, as entidades abrangidas dividem-se entre entidades essenciais e entidades importantes;
- Maior precisão e reforço das medidas de gestão dos riscos de cibersegurança a adotar pelas entidades;
- Consideração da cibersegurança da cadeia de abastecimento;
- Regras mais detalhadas, específicas e otimizadas quanto ao reporte de incidentes de cibersegurança;
- Maior especificação dos poderes de supervisão das autoridades de cibersegurança;
- Atribuição de responsabilidade às pessoas singulares responsáveis por entidades abrangida e preocupação na sua formação em cibersegurança;
- Quadro sancionatório harmonizado a nível da União Europeia, mais robusto e com coimas mais elevadas.

3.10. *Cyber Resilience Act*

O CRA (*Cyber Resilience Act*) é uma diretiva legal europeia que impõe um conjunto de requisitos e obrigações que irão forçar todos os fabricantes, programadores de *software*, importadores, fornecedores e outras partes envolvidas no fornecimento de produtos digitais no espaço europeu, a encarar a segurança de forma séria e eficiente.

A aplicação do CRA a todo o ciclo de vida desta categoria de produtos, obriga os intervenientes a incluir medidas efetivas de cibersegurança ou fazer uso de práticas de desenvolvimento seguro que vão desde a segurança por *design* e por construção até à proteção de dados pessoais (indo ao encontro do RGPD), passando também pela gestão de riscos e gestão de incidentes, conduzindo assim toda a cadeia de fornecimento a apresentar processos de mitigação rápidos e eficientes no tratamento de vulnerabilidades e outras questões relacionadas com a segurança dos seus produtos.

Também no contexto do CRA, se um fabricante tomar conhecimento de um risco de cibersegurança, deve tomar medidas imediatas para resolvê-lo, incluindo notificar os utilizadores e os CSIRT dentro de um curto prazo. Nestes casos, devem também cooperar com as autoridades nacionais na investigação e resolução de incidentes de cibersegurança relacionados com os seus produtos.

Estas diretivas vêm complementar todo um conjunto de outras leis e medidas que, isoladas, abordavam ou mitigavam problemas específicos.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

3.10.1. Qual é a legislação aplicável?

Não existindo ainda transcrição desta diretiva para a legislação portuguesa, fica indicada como referência a diretiva aprovada pelo parlamento europeu.

3.10.2. Qual é a motivação desta medida?

Hoje em dia, os principais vetores usados em ataques cibernéticos assentam em vulnerabilidades e falhas presentes em produtos de *hardware* e *software*.

No mundo global em que vivemos, com organizações ligadas em rede e à rede global, um incidente de cibersegurança com um único produto tende a afetar toda a organização, podendo propagar-se rapidamente a toda a cadeia de fornecedores e clientes e, no limite, propagar-se a todo o país ou mesmo para fora das fronteiras, em poucos minutos.

É por isso fundamental ter controlo e ter também possibilidade de atuar rapidamente sobre todas as vulnerabilidades ou falhas que se vão identificando ou que vão sendo apontadas pelos investigadores da área. Neste contexto, políticas efetivas de reação por parte dos fabricantes ou dos desenvolvedores de *software*, são fundamentais.

Sendo confrontados com produtos atualizáveis e passíveis de receber correções que resolvam vulnerabilidades que possam surgir e com toda a informação relevante sobre as características de cibersegurança dos produtos, os seus consumidores ficarão mais aptos a fazer escolhas mais informadas e seguras.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027
Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

4. Atualização de *Software* e *Patches*

Na era da informação, a era em que vivemos, o uso de dispositivos eletrónicos, como computadores e telemóveis, tornou-se essencial. Todos os dispositivos que são utilizados diariamente assentam o seu funcionamento em sistemas operativos e aplicações. Sistemas esses que funcionam com *software* e foram desenvolvidos e implementados por seres humanos, e, como tal, podem ter *bugs*, que posteriormente são detetados e corrigidos.

As **atualizações de *software* e os *patches*** [20, 21, 22, 23, 24] são, por isso, práticas **cruciais** para a segurança dos sistemas.

Enquanto os *bugs* não são corrigidos, estes podem levar a dois tipos de situações distintas:

- **Mau funcionamento do sistema ou da aplicação**, podendo levar a resultados inesperados nos mesmos;
- Mesmo que o sistema esteja a funcionar bem, o *bug* poderá já ter sido explorado por alguém que possa já ter detetado esse *bug* anteriormente. Essa falha pode ser utilizada de forma camuflada para comprometer as credenciais ou outras informações que estejam no sistema em causa. Este uso indevido pode chegar ao ponto do **sistema da vítima** estar a ser utilizado para **escutar ou roubar** credenciais de outros intervenientes que se liguem na mesma rede.

Os *patches* corrigem estas vulnerabilidades e protegem contra ameaças cibernéticas. Uma atualização de *software* melhora a funcionalidade, experiência do utilizador, corrige problemas, introduz novas funcionalidades e otimiza o desempenho. À medida que o tempo passa, as vulnerabilidades vão sendo descobertas e são corrigidas pelos desenvolvedores de *software*.

Apesar de muitas vezes ser um incómodo atualizar o *software*, ignorar estas atualizações pode ter consequências graves, visto que as vulnerabilidades já conhecidas são frequentemente exploradas por *hackers* para ter acesso a sistemas, como explicado também em cima.

De seguida são apresentadas algumas razões pelas quais é **importante a atualização do *software***:

- **Corrigir falhas de segurança:** a segurança é a principal razão para atualizar o *software* imediatamente. As vulnerabilidades do *software* podem ser vistas como portas abertas para que *hackers* entrem num computador e, por exemplo, instalem *malware* nos sistemas. Os *patches* de segurança bloqueiam estas portas no *software* e protegem um dispositivo contra ataques;
- **Obter novas funcionalidades:** a atualização do *software*, por norma, acrescenta novas funcionalidades e pode remover antigas que já não são necessárias;
- **Proteger os dados:** a atualização do *software* permite mitigar as vulnerabilidades de segurança, o que permite uma melhor proteção dos dados;
- **Melhorar o desempenho:** nem todos os *patches* estão relacionados com a segurança. Podem ser encontrados erros num programa, ou pode ser necessário melhorar um programa, e há *patches* que ajudam nisso mesmo, levando num final a uma melhoria no desempenho do *software*;
- **Garantir a compatibilidade:** os "fornecedores" de *software* enviam atualizações de modo a garantir que o seu *software* é compatível com a tecnologia mais recente, visto que podem existir erros de compatibilidade caso isto não seja feito.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

Algumas **dicas para a atualização do *software*** são as seguintes:

- **Configurar as atualizações automáticas:** hoje em dia, a maioria dos programas já disponibiliza a opção de atualizações automáticas, e esta é a forma mais fácil de manter o *software* atualizado sem ter de ser procurar por estas atualizações manualmente;
- **Procurar por atualizações regularmente:** se preferir atualizar o *software* manualmente, então deve procurar-se com regularidade se existem atualizações;
- **Atualizar todo o *software*:** não se deve apenas atualizar o sistema operativo, mas também todo o *software* e aplicações que estão num dispositivo.

É necessário ter em atenção os falsos esquemas de atualização. Estes são um tipo de ataques em que os atacantes tentam induzir o utilizador a descarregar e instalar um ficheiro malicioso que finge ser uma atualização de software. A melhor maneira de evitar estes esquemas é nunca fazer efetuar *download* ou instalar atualizações de *software* a partir de fontes não conhecidas ou suspeitas.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

5. Palavras-Passe Seguras

Uma palavra-passe [25] serve como mecanismo de autenticação, demonstrando conhecimento de um segredo que permite autenticar o utilizador. São as palavras-passe que protegem as contas e dispositivos eletrónicos contra o acesso não autorizado, e ajudam a manter as informações sensíveis. A **complexidade** da palavra-passe **tem um papel crucial**, visto que quanto mais complexa esta for, mais difícil é de descobrir e mais protegidas estarão as informações contra ameaças informáticas e *hackers*. Em baixo encontram-se alguns aspetos a ter em conta aquando a criação de uma senha segura:

- **Complexidade das palavras-passe:** as palavras-passe devem ser complexas, isto é, devem ter pelo menos 12 caracteres de comprimento [26], e uma combinação entre letras maiúsculas, minúsculas e caracteres especiais. Deve evitar-se o uso de informações pessoais, como a data de nascimento, nome, entre outros;
- **Uso de palavras-passe únicas:** não se deve reutilizar as palavras-passe em várias contas, visto que se uma palavra-passe for comprometida, o impacto causado poderá ser menor;

Outro aspeto importante é o uso de **Autenticação de Dois Fatores** (ou *Two Factor Authentication (2FA)*). Esta é uma medida de segurança essencial que adiciona uma camada adicional de proteção para além do uso de palavras-passe seguras. A 2FA **requer um segundo fator de autenticação**, como por exemplo um código enviado por SMS, por *email* ou então um código gerado por uma aplicação que gera tokens para este efeito.

O uso da autenticação de dois fatores é bastante importante, porque se uma senha for comprometida e essa conta tiver implementado este mecanismo, o risco da conta estar comprometida é menor.

Este método é bastante fácil de implementar, visto que muitos dos serviços já oferecem opções de 2FA integradas, e a sua configuração a partir daí é simples. **Incentiva-se o uso da 2FA em todas as contas**, mas em especial em **contas sensíveis** e mais **importantes**, como por exemplo contas de email, contas em sistemas financeiros, etc.

Para além das dicas acima indicadas, existem ainda comportamentos a **evitar**, de onde se destacam os seguintes:

- A **utilização das mesmas palavras-passe em diferentes contas** é uma prática a evitar, visto que uma vez descoberto uma dessas senhas, múltiplas plataformas e contas poderão ficar comprometidas;
- A **escrita de palavras-passe em papel** é uma má prática, mesmo que se usem mecanismos de disfarce, esta prática não é segura e não deve ser usada;
- Outra abordagem bastante frequente é a **escrita das palavras-passe em documentos de texto ou folhas de cálculo**, que apesar de ser mais segura que as anteriores, deve ser evitada, visto que este ficheiros podem de igual forma ser acedidos.
- O armazenamento de credenciais no *browser* não é uma boa prática, já que a maioria dos *browsers* não ter capacidades de autenticação de dois ou vários fatores incorporadas, o que significa que tudo o que um intruso teria de fazer era aceder ao seu dispositivo.

Visto que cada vez são utilizadas mais aplicações e sistemas, é difícil decorar todos as palavras-passe, principalmente se estas forem complexas (como deveriam ser). Para solucionar isto, e para evitar os comportamentos acima, devem ser utilizados **Gestores de Palavras-Passe**.

Um gestor de palavras-passe é bastante útil para armazenar as mesmas de forma segura, preencher automaticamente as credenciais de *login* quando necessário e também podem gerar palavras-passe fortes (onde se pode alterar o tamanho da senha, o uso de caracteres especiais, entre outros).

A lista abaixo apresenta várias sugestões de gestores de palavras-passe:

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

- **Bitwarden**;
- **Proton Pass**;
- **KeePass**;
- **1Password**.

Para garantir uma boa gestão de credenciais e acessos, é **essencial questionar qualquer solicitação** de fornecimento de dados de acesso que ocorra fora do contexto normal de uso das aplicações. Mesmo que o pedido pareça legítimo, seja por e-mail ou qualquer outro meio, os responsáveis pela gestão dos recursos ou aplicações nunca precisam de conhecer as credenciais dos utilizadores. Portanto, estes dados **nunca devem ser partilhados com terceiros**.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

6. Controlo de Acesso

O **controlo de acesso** [27, 28, 29] é uma componente fundamental na segurança dos dados. Este determina quem tem **permissão para aceder a determinados dados**, aplicações e recursos e em que circunstâncias. Da mesma forma que as chaves e as listas de convidados pré-aprovados protegem os espaços físicos, **as políticas de controlo de acesso protegem os espaços digitais**. As políticas de controlo de acesso baseiam-se fortemente em técnicas como a autenticação e a autorização, que permitem às organizações verificar explicitamente se os utilizadores são quem dizem ser e se lhes é concedido o nível de acesso adequado com base no contexto, como o dispositivo, a localização, a função, entre outros. O controlo de acesso evita que informações confidenciais sejam roubadas por agentes mal-intencionados ou outros utilizadores não autorizados.

Em vez de gerir as permissões manualmente, a maioria das organizações orientadas para a segurança apoiam-se em soluções de gestão de identidade e acesso para implementar políticas de controlo de acesso.

Há **quatro tipos principais de controlo de acesso**, cada um dos quais administra o acesso a informações sensíveis de uma forma única:

- **Controlo de Acesso Discricionário** (*Discretionary Access Control (DAC)*) – neste tipo de modelo, cada objeto de um sistema protegido tem um proprietário e os proprietários concedem acesso aos utilizadores à sua descrição. O DAC proporciona um controlo caso-a-caso dos recursos;
- **Controlo de Acesso Obrigatório** (*Mandatory Access Control (MAC)*) – neste tipo de modelo, o acesso é concedido aos utilizadores sob a forma de uma autorização. Uma autoridade central regula os direitos de acesso e organiza-os em níveis, que se expandem uniformemente em termos de âmbito. Este modelo é muito comum em contextos governamentais e militares;
- **Controlo de Acesso Baseado na Função** (*Role-Based Access Control (RBAC)*) – neste tipo de modelo, os direitos de acesso são concedidos com base nas funções comerciais definidas, em vez da identidade ou grau de experiência dos indivíduos. O objetivo é fornecer aos utilizadores apenas os dados de que necessitam para desempenhar as suas funções – e nada mais;
- **Controlo de Acesso Baseado em Atributos** (*Attribute-Based Access Control (ABAC)*) – neste tipo de modelo, o acesso é concedido de forma flexível, com base numa combinação de atributos de controlo de acesso mais granular e ajuda a reduzir o número de atribuições de funções.

6.1. Melhores práticas de Controlo de Acesso

Há algumas práticas que se devem ter em conta quando se implementa o controlo de acesso. Esta secção mostra as melhores práticas de controlo de acesso.

- **Atribuir os direitos de acesso de acordo com as funções do utilizador**

O **controlo de acesso baseado em funções** simplifica o desafio complexo do controlo de acesso e aumenta a segurança. As configurações deste tipo de controlo de acesso associam funções organizacionais a privilégios de acesso adequados.

Os sistemas de acesso baseados em funções melhoram a eficiência operacional. Não é necessário atribuir direitos de acesso a funcionários individuais. **As novas contratações recebem privilégios de acordo com a sua função na organização**. As ferramentas automatizadas fornecem os privilégios corretos, e podem eliminar direitos de acesso obsoletos quando os trabalhadores ou mudam de funções ou saem da organização.

O controlo de acesso baseado em funções também ajuda a evitar o problema de contas partilhadas. Os utilizadores partilham frequentemente contas para gerir projetos ou aceder a ferramentas administrativas, o que é extremamente inseguro e pode expor toda a rede a

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

ataques externos. Para contornar este problema, a definição clara das funções dos utilizadores e garantir que cada utilizador pode aceder às ferramentas de que necessita.

- **Utilizar o princípio do menor privilégio para orientar o controlo de acesso**

O **princípio do menor privilégio** é um conceito crítico de gestão de acesso. De acordo com esta ideia, **os utilizadores da rede devem ter um acesso mínimo aos dados e aplicações**. Os utilizadores devem poder aceder aos recursos necessários para as suas tarefas profissionais, mas, tudo o resto está fora de alcance.

A **restrição do acesso dentro dos limites da rede é um aspeto fundamental dos sistemas de cibersegurança**. Se os atacantes obtiverem acesso, não podem mover-se facilmente dentro da rede. As equipas de segurança podem conter as ameaças e proteger mais facilmente os sistemas sensíveis.

- **Desenhar um sistema de controlo de acesso com vários níveis**

Os controlos baseados em funções e os princípios de acesso mínimo são apenas parte do desafio do controlo de acesso. A **autenticação** e as **camadas de segurança da rede** também ajudam a **controlar o acesso e a proteger os recursos**. Isto reforça o limite da rede e reduz o risco de entrada maliciosa.

Implementar a autenticação multifator (em inglês, Multi-Factor Authentication (MFA)) para ativos críticos. A MFA requer mais do que um fator de autenticação antes de permitir o acesso, tornando muito mais difícil violar as defesas da rede.

As *firewalls* e as listas de controlo de acesso conferem uma resiliência adicional aos controlos de acesso, e também é possível combinar controlos baseados em funções com controlos baseados em atributos. Isto permite que as equipas de *Information Technologies (IT)* adicionem proteção adicional aos ativos críticos.

A formação acrescenta outra camada de segurança. É importante que os trabalhadores recebam formação sobre a higiene das palavras-passes e trabalho remoto seguro. Para além disso, também é importante que também se saiba como funcionam os controlos de acesso.

- **Compreender o ambiente do utilizador**

O controlo de acesso baseia-se no conhecimento. As organizações precisam de saber **quem está a utilizar os seus sistemas**, **quando os utilizam e que recursos utilizam**.

É importante criar e manter uma base de dados de utilizadores abrangente. **Cada perfil de utilizador deve conter informações claras sobre a função do utilizador na organização**, que deve ser refletida com os seus privilégios de acesso de acordo com as políticas de controlo. A gestão de utilizadores também se aplica a terceiros. E também se aplica a clientes e consumidores.

Evite a duplicação de contas de utilizador e remova os perfis não utilizados quando os funcionários saem. Os utilizadores autorizados devem ser identificados de forma única. Isto permite autenticá-los de forma segura e acompanhar a sua atividade enquanto utilizam os recursos da empresa.

- **Gerir continuamente o sistema de acesso**

A automatização reduz a carga de trabalho do controlo de acesso, mas, independentemente disso, quem está responsável pela segurança tem de continuar a monitorizar os padrões de acesso dos utilizadores. Além disso, têm de se efetuar auditorias regulares para garantir que os controlos de acesso estão a funcionar corretamente.

As melhores práticas incluem a orientação das auditorias para tarefas importantes de controlo de acesso:

- As auditorias técnicas **identificam problemas de experiência do utilizador**. Isto permite aos administradores otimizar os privilégios e os processos de autenticação;
- As auditorias de segurança **identificam alertas e potenciais ataques**, e sugerem formas de reforçar os controlos de recursos críticos;
- As auditorias de contas **verificam se existem contas órfãs**, **privilégios partilhados** ou **níveis de acesso indevidamente elevados**.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

6.2. Conselhos sobre como implementar o controlo de acesso

- **Dica 1 - Centralizar a gestão de acesso**

Evite utilizar de forma regular listas de controlo de acesso geridas pelos proprietários dos recursos. Isto torna mais difícil limitar os privilégios dos utilizadores. Em vez disso, crie uma base de dados central de direitos de acesso antes de implementar controlos de acesso.

A centralização facilita o controlo dos privilégios associados a funções ou indivíduos. Os administradores podem fornecer políticas de acesso a todos os utilizadores e alterar as definições instantaneamente. Podem adicionar controlos baseados em atributos a documentos ou dados e adicionar ou remover utilizadores facilmente.

- **Dica 2 - Automatizar a desvinculação para melhorar a segurança**

Os privilégios dos utilizadores devem terminar quando os funcionários deixam uma organização. Mas sem uma gestão adequada, os perfis podem permanecer ativos durante semanas ou meses. Os atacantes externos aproveitam os perfis órfãos para montar ataques que são muito difíceis de detetar. Por isso, é importante remover todos os privilégios imediatamente.

A gestão automatizada de perfis resolve este problema. Ligue os seus controlos de acesso a sistemas que removem todos os direitos de utilizador. Isto estende-se para além dos recursos de rede no local, para serviços na nuvem, aplicações de terceiros e barreiras de controlo de acesso físico.

- **Dica 3 - Considerar controlos de acesso flexíveis**

Os utilizadores podem necessitar de acesso temporário a bases de dados específicas, ou podem necessitar de privilégios de escrita para editar documentos que normalmente lhes são negados. Quem está encarregue pela segurança pode querer delimitar geograficamente os recursos se estiver preocupado com ataques de um determinado país.

Os controlos baseados em funções tendem a ser bastante inflexíveis. Mas os administradores podem complementar o RBAC com controlos granulares, conforme necessário. Os controlos baseados no contexto têm em conta a localização, os tipos de dispositivos, o tempo de acesso e muitos outros fatores.

- **Dica 4 - Certificar-se que os sistemas de acesso dispõem de ferramentas de criação de relatórios**

O controlo de acesso é uma parte importante das estratégias de conformidade. Mas os controlos são inúteis se não gerarem provas que possam ser consultadas pelos reguladores. Escolha sistemas com funções de auditoria que registem todos os eventos de acesso.

As ferramentas automatizadas baseadas em regras criam relatórios que são adaptados às necessidades regulamentares. Por exemplo, um retalhista de comércio eletrónico pode necessitar de dados sobre o acesso às informações do titular do cartão. Um sistema de controlo de acesso sólido fornecerá estas informações a pedido.

- **Dica 5 - Sistemas de acesso nativos da nuvem**

As empresas modernas dependem frequentemente de ferramentas SaaS para armazenar informações, partilhar documentos e gerir dados de clientes. Os funcionários podem criar novos recursos na nuvem num instante, por vezes sem o conhecimento das equipas de IT.

Implemente sistemas que descubram automaticamente novas aplicações na nuvem. E facilite a ligação das aplicações na nuvem aos sistemas de acesso existentes. O seu registo de identidade central deve ser compatível com a nuvem. E todas as aplicações na nuvem devem estar sujeitas aos seus controlos de autorização. Desta forma, pode proteger a sua arquitetura de rede e tirar partido das vantagens da computação em nuvem.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

7. Sistemas de Monitorização de Redes

Os **sistemas de monitorização de redes** [30, 31, 32] incluem ferramentas de *software* e *hardware* que podem acompanhar vários aspetos de uma rede e do seu funcionamento, como o tráfego, a utilização da largura de banda (isto é, a taxa a que os dados fluem na rede) e o tempo de atividade. Estes sistemas podem **detetar dispositivos** e outros elementos que compõem ou tocam a rede, bem como fornecer atualizações de estado. Os administradores de rede confiam neste tipo de sistema para os ajudar a **detetar rapidamente falhas de dispositivos ou ligações ou problemas**, como congestionamento de tráfego que limita o fluxo de dados. A capacidade de detetar problemas estende-se a partes da rede tradicionalmente para além dos seus limites de demarcação. Estes sistemas podem alertar os administradores para os problemas por correio eletrónico e apresentar relatórios utilizando a análise da rede.

7.1. Intrusion Detection System

Um **sistema de deteção de intrusões** [33, 34] (em inglês, *Intrusion Detection System (IDS)*) é uma ferramenta de segurança de rede que **monitoriza o tráfego de rede** e os **dispositivos** para **detetar atividades maliciosas conhecidas, atividades suspeitas** ou **violações da política de segurança**.

Um IDS pode ajudar a acelerar e automatizar a deteção de ameaças à rede, alertando os administradores de segurança para ameaças conhecidas ou potenciais, ou enviando alertas para uma ferramenta de segurança centralizada. Uma ferramenta deste tipo pode combinar dados de outras fontes para ajudar as equipas de segurança a identificar e responder a ciberameaças que possam escapar a outras medidas de segurança.

Um IDS **não pode impedir as ameaças à segurança por si só**. Atualmente, as capacidades de um IDS são integradas ou incorporadas em Sistema de Prevenção de Intrusões.

7.2. *Intrusion Prevention System*

Um **sistema de prevenção de intrusões** [35, 36] (em inglês, *Intrusion Prevention System (IPS)*) **monitoriza o tráfego de rede** para **detetar potenciais ameaças** e **bloqueia-as automaticamente**, alertando a equipa de segurança, terminando ligações perigosas, removendo conteúdos maliciosos ou acionando outros dispositivos de segurança.

As soluções IPS evoluíram a partir dos IDS; um sistema deste tipo tem as mesmas funções de deteção e comunicação de ameaças que um IDS, além de capacidades de prevenção automatizada de ameaças.

7.3. *Endpoint Detection and Response*

A **deteção e resposta de ponto de extremidade** [37, 38, 39] (em inglês *Endpoint Detection System (EDR)*) é um *software* que utiliza **análise em tempo real** e automatização orientada por Inteligência Artificial (*Artificial Intelligence (AI)*) para proteger os utilizadores, os dispositivos terminais e os ativos de uma organização contra ciberameaças que ultrapassam o antivírus ou outras ferramentas tradicionais de segurança de endpoints.

Um EDR **analisa os dados**, e, caso identifique algo suspeito, pode **responder automaticamente** para **prevenir** ou **minimizar** danos das ameaças que possa encontrar.

7.4. *Security Information and Event Management*

A **Gestão de Informação e Eventos de Segurança** [40, 41] (em inglês, *Security Information and Event Management (SIEM)*) é uma **solução** de segurança que ajuda as organizações a **reconhecer** e a **abordar** potenciais **ameaças** e vulnerabilidades de segurança antes destas terem oportunidade de perturbar as operações comerciais. Os sistemas SIEM ajudam

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027
Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

as equipas de segurança das empresas a detetar anomalias no comportamento dos utilizadores e utilizam AI para automatizar muitos dos processos manuais associados à deteção de ameaças e à resposta a incidentes.

7.5. Principais Vantagens de Sistemas de Monitorização de Redes

As **principais vantagens** das empresas utilizarem sistemas de monitorização de redes são as seguintes:

- **Visibilidade clara da rede** - através da monitorização da rede, os administradores podem obter uma imagem clara de todos os dispositivos ligados na rede. É possível também ver como os dados se estão a mover entre os dispositivos e identificar e corrigir rapidamente os problemas que possam prejudicar o desempenho e levar a interrupções;
- **Complexidade crescente** - as empresas modernas dependem de uma série de serviços críticos para os negócios e dependentes da Internet. Isto inclui fornecedores de serviços na nuvem, provedor de serviços de Internet, entre outros. Cada serviço opera através da Internet, tornando-o suscetíveis a flutuações de desempenho causadas por interrupções na Internet ou problemas de encaminhamento. A visibilidade dos componentes de rede fora do seu controlo permite-lhe monitorizar os problemas que podem afetar os funcionários ou os clientes;
- **Melhor utilização dos recursos de IT** - as ferramentas de *hardware* e *software* dos sistemas de monitorização da rede reduzem o trabalho manual das equipas de IT. Isto significa que o valioso pessoal de IT tem mais tempo para se dedicar a projetos críticos para a organização;
- **Visão antecipada das futuras necessidades de infraestruturas** - os sistemas de monitorização de rede podem fornecer relatórios sobre o desempenho dos componentes da rede durante um período definido. Ao analisar estes relatórios, os administradores de rede podem antecipar quando é que a organização pode ter de considerar a atualização ou a implementação de uma nova infraestrutura de IT;
- **Capacidade de identificar ameaças à segurança mais rapidamente** - a monitorização de rede ajuda as organizações a compreenderem o que é um desempenho normal das suas redes. Assim, quando ocorre uma atividade invulgar, como um aumento inexplicável dos níveis de tráfego de rede, é mais fácil para os administradores identificarem rapidamente o problema, e determinarem se pode ser uma ameaça à segurança.

7.6. Protocolos de Monitorização de Redes

Já anteriormente neste guia foi feita uma breve explicação de Protocolos de Monitorização de Redes. Caso queira ver novamente a explicação dos mesmos, pode ver novamente a secção 2.3.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

8. *Backup* e Recuperação de Dados

Cópias de segurança, ou *backups*, [42, 43, 44, 45] e a **recuperação de dados**, juntos, englobam o **processo de duplicar dados e armazená-los** num local seguro, para que, em caso de perda ou danos seja possível restaurar esses dados para que estes possam ser utilizados novamente. Idealmente, este *backup* deve ser imutável, ou seja, não deverá ser alterado depois de ser criado, de modo a proteger contra mutações, como por exemplo, *ransomware* [1] e ataques.

É importante de realçar que os sistemas de *backup* de dados apenas devem ser ligados no momento de efetuar a cópia, e desligados de seguida.

A principal **diferença** entre uma cópia de segurança e a recuperação de dados é que o processo de *backup* é uma forma de **guardar** e **proteger** os dados e de os **armazenar em segurança** para os ter mais tarde, caso sejam necessários. A **recuperação** é o processo através do qual se **recuperam** e **restauram** os dados da cópia de segurança para os sistemas em produção. As cópias de segurança fiáveis e a recuperação rápida garantem a continuidade e a resiliência do negócio.

Porque é que a cópia de segurança e a recuperação de dados são importantes?

Os dados são algo essencial em cada organização, e podem apresentar uma vantagem competitiva. A principal função de um *backup* e recuperação de dados, e, talvez, a mais importante, é a **preservação dos dados críticos** em caso de perdas ou danos. Para além disso, perante uma catástrofe, é só com uma estratégia deste tipo que se conseguem manter as operações, manter a empresa a funcionar. Outras razões pelo qual é importante ter um plano destes é para conservar registos, que podem também ser importantes a nível jurídico.

Desenvolver uma estratégia de *backup* e recuperação de dados é **essencial**. Uma base de dados pode ficar inutilizável devido a uma falha de *hardware* ou de *software*, ou ambas. Poderá também deparar-se com problemas de armazenamento, interrupções de energia ou outras falhas, e cada cenário de falha requer uma ação de recuperação de dados diferentes, daí ser bastante importante a existência de uma estratégia de recuperação de dados bem delineada.

8.1. Tipos de *Backup* de Dados

Avaliar que tipo de cópia de segurança se adequa a determinadas necessidades empresariais é bastante prudente.

Existem três tipos principais de *backups* para efetuar cópias de segurança de ativos digitais:

- ***Full Backup*** (cópia de segurança total) - o método mais básico e abrangente, em que todos os dados são enviados para outro local;
- ***Incremental Backup*** (cópia de segurança incremental) - é feito o *backup* de todos os arquivos que foram alterados desde o último *backup*;
- ***Differential Backup*** (cópia de segurança diferencial) - é feito o *backup* apenas de cópias de todos os ficheiros que foram alterados desde o último *backup* completo.

Nem todas as organizações conseguem suportar todos os tipos de *backups*, uma vez que a capacidade da rede pode variar de organização para organização.

A escolha do método de *backup* correto requer uma abordagem tática - uma escolha que possa ajudar as organizações a obter o melhor nível de proteção de dados sem exigir demasiado da rede. No entanto, antes de determinar qual é o método de cópia de segurança que melhor se adequa às necessidades de uma empresa, é conveniente compreender os prós e contras dos três principais tipos de cópia de segurança acima mencionados.

[1] O *ransomware* é um tipo de *malware* que mantém os dados sensíveis ou o dispositivo da vítima como reféns, ameaçando mantê-los bloqueados (ou pior que isso) caso a vítima não pague um resgate ao atacante.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

Full Backup

Uma cópia de segurança completa envolve a criação de uma cópia completa dos ficheiros, pastas, dados e discos rígidos de uma organização. É a proteção perfeita contra a perda de dados quando se tem em conta a velocidade e a simplicidade da recuperação. No entanto, o tempo e as despesas necessárias para copiar todos os dados podem tornar esta opção indesejável para muitas organizações.

Aqui estão as vantagens de executar um *full backup*:

- Tempo de restauro rápido;
- A gestão do armazenamento é fácil visto que todos os dados são armazenados numa única versão;
- O controlo fácil da versão permite manter e restaurar diferentes versões sem esforço;
- A pesquisa de ficheiros é muito fácil.

As desvantagens de executar um *full backup* estão listadas abaixo:

- Exige, comparativamente com outros métodos, um maior espaço de armazenamento;
- Dependendo do seu tamanho, pode demorar muito tempo a fazer cópias de segurança dos ficheiros;
- A necessidade de espaço de armazenamento adicional torna-o o método de *backup* mais dispendioso;
- O risco de perda de dados é elevado, uma vez que todos os dados são armazenados num único local.

Em que situações deve ser feito um *full backup*? As pequenas empresas, que lidam consistentemente com uma pequena quantidade de dados, podem considerar o *backup* completo uma boa opção, uma vez que não consome muito espaço de armazenamento nem demora muito tempo a efetuar a cópia de segurança.

Incremental Backup

O *backup* incremental envolve o *backup* de todos os arquivos, pastas, dados e discos rígidos que foram alterados desde a última atividade de *backup*. Apenas as alterações mais recentes são objeto das cópias de segurança, consumindo menos espaço de armazenamento e resultando numa cópia de segurança rápida. Porém, o tempo de recuperação é mais longo, uma vez que será necessário aceder a mais ficheiros de *backup*.

Os prós deste método são os seguintes:

- Utilização eficiente do espaço de armazenamento, uma vez que os ficheiros não são duplicados na sua totalidade;
- Cópias de segurança extremamente rápidas;
- Pode ser executado com a frequência desejada, sendo que cada incremento é um ponto de recuperação individual.

Já os contras do *incremental backup* são os seguintes:

- O restauro é demoroso, uma vez que os dados têm de ser reunidos a partir de várias cópias de segurança;
- A recuperação bem sucedida só é possível se todos os ficheiros de *backup* forem à prova de danos;

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

- A pesquisa de ficheiros é complicada - é necessário procurar em mais do que um conjunto de cópias de segurança para restaurar um ficheiro específico.

Quando é que se deve utilizar o *backup* incremental? As empresas que lidam com grandes volumes de dados e que não podem dedicar tempo ao processo de cópias de segurança considerarão os métodos de cópia de segurança incremental eficazes, uma vez que ocupam menos espaço de armazenamento e promovem cópias de segurança rápidas.

Differential Backup

O *backup* diferencial situa-se entre o *backup* completo e o *backup* incremental. Este método envolve o *backup* de ficheiros, pastas e unidades de disco rígido que foram criados ou alterados desde o último *backup* completo. É apenas efetuado o *backup* de um pequeno volume de dados entre o intervalo de tempo do último *backup* e o atual, consumindo menos espaço de armazenamento e exigindo menos tempo e investimento.

As vantagens de um *differential backup* estão listadas abaixo:

- Ocupa menos espaço do que os *backups* completos;
- Restauro mais rápido do que as cópias de segurança incrementais;
- Cópias de segurança muito mais rápidas do que as cópias de segurança completas.

Já os contras são os seguintes:

- Possibilidade de recuperação falhada se algum dos conjuntos de cópias de segurança estiver incompleto;
- Em comparação com as cópias de segurança incrementais, a cópia de segurança demora mais tempo e requer mais espaço de armazenamento;
- Em comparação com o *backup* completo, o restauro é lento e complexo.

Quando é que deve utilizar o backup diferencial? As organizações de pequena e média dimensão que pretendam processar grandes volumes de dados valiosos, mas que não possam efetuar cópias de segurança constantes, considerarão útil o método de cópia de segurança diferencial.

8.2. Periodicidade de *Backups*

A frequência das cópias de segurança depende da importância dos dados e da frequência com que esses dados são alterados [46].

Idealmente, devem ser efetuados *backups* dos dados regularmente, por exemplo, diariamente, semanalmente ou mensalmente, de acordo com os tipos de dados.

Os ficheiros importantes e que são frequentemente modificados podem exigir cópias de segurança mais frequentes para evitar uma potencial perda de dados.

8.3. Regra de *Backup* 3 2 1

A **Regra de *Backup* 3 2 1** [47] foi feita para ajudar a simplificar os procedimentos de *backup* e reduz o risco de perda de dados. Esta regra ajuda a recuperar rapidamente os dados e retomar as operações, pois mantém o tempo de inatividade mínimo.

Esta regra envolve duplicar os dados três vezes, armazená-los em dois dispositivos distintos e ter uma cópia dos dados fora do local.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

Três Cópias de Dados

O primeiro elemento da regra de *backup* 3 2 1 enfatiza ter três cópias de segurança dos dados. Esta redundância garante que, mesmo que uma cópia fique inacessível ou corrompida, ainda existem duas cópias adicionais disponíveis para restauração dos dados. Ao manter várias cópias, o risco de perda permanente de dados é reduzido significativamente.

Dois Dispositivos Diferentes

O segundo aspeto da regra de *backup* 3 2 1 sugere armazenar cópias em dois formatos ou dispositivos diferentes. Esta diversificação fornece uma camada adicional de proteção contra tipos específicos de falhas.

Por exemplo, ter uma cópia num disco rígido externo físico e outra cópia na nuvem, os dados ficam protegidos contra falhas de *hardware* e falhas de segurança *online*. A diversificação dos dispositivos de armazenamento minimiza as chances de se perderem todas as cópias simultaneamente.

Uma cópia Armazenada Fora do Local

Ó último elemento da regra de *backup* 3 2 1 é manter uma cópia dos dados fora do local. Esta cópia de segurança deverá estar noutro local fora da área principal onde os dados são criados ou mantidos.

Este ponto ajuda a proteger os *backups* contra perigos físicos, como incêndios, inundações, roubos ou outras catástrofes que possam afetar o local onde a cópia de segurança está armazenada.

Esta regra estabelece uma base sólida que equilibra a diversidade, redundância e armazenamento externo, assegurando a disponibilidade e resiliência de informações fundamentais. Por isso, este é um método confiável para as organizações que desejam melhorar os seus métodos de *backup* de dados.

Ao longo da explicação da regra já foram mencionados alguns benefícios da implementação desta regra. Abaixo apresenta-se uma lista com os principais benefícios desta regra:

- Redundância de dados e proteção contra falhas de *hardware*;
- Mitigação de riscos de perda de dados;
- Recursos aprimorados de recuperação após desastres;
- Proteção contra ataques de *ransomware*.

Não seguir a regra de *backup* de dados 3 2 1 expõe as organizações a ramificações desnecessárias e significativas, incluindo:

- Vulnerabilidade à perda e corrupção de dados;
- Aumento do impacto dos desastres naturais;
- Maior suscetibilidade a ataques de *ransomware*.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

9. Plano de Recuperação de Desastres

Um **Plano de Recuperação de Desastres** (ou *Disaster Recovery Plan (DRP)*) [48, 49] é um documento detalhado que descreve como uma organização deverá atuar de forma eficaz a um incidente não planeado e retomar as operações. Estes planos ajudam a garantir que as empresas estão preparadas para enfrentar diferentes tipos de desastres, incluindo falhas de energia, ataques de *ransomware* e *malware*, desastres naturais, entre outros.

Um DRP sólido ajuda a **rápida e eficazmente a restaurar a conetividade** e a reparar a perda de dados após uma catástrofe.

Tal como um DRP, um **Plano de Continuidade Empresarial** (ou *Business Continuity Plan (BCP)*) faz parte do processo de recuperação de desastres que ajuda as empresas a restaurar as operações normais após a ocorrência de um desastre. Normalmente, os BCPs têm uma visão mais ampla das ameaças e das opções de resolução do que os DRPs, concentrando-se no que uma empresa precisará para restaurar as funções comerciais básicas após um incidente.

Já um **Plano de Resposta a Incidentes** (ou *Incident Response Plan (IRP)*) são um tipo de plano de recuperação de desastres que se centram exclusivamente na **cibersegurança** e nas **ameaças aos sistemas de informação**.

Um IRP descreve claramente a resposta de emergência de uma organização desde o momento em que deteta uma ameaça até à sua mitigação e resolução. Um plano deste tipo procura abordar os danos específicos causados por um ciberataque e centra-se exclusivamente na preparação para ameaças à tecnologia, à infraestrutura de IT, às operações comerciais e à reputação.

9.1. Importância de um Plano de Recuperação de Desastres

Os Planos de Recuperação de Desastres desempenham um **papel fundamental** no desenvolvimento de um plano de segurança global que ajuda a garantir às partes interessadas, clientes e investidores que uma empresa funciona de forma responsável. As empresas que não tomam as medidas necessárias para garantir a preparação enfrentam vários riscos, incluindo perda de dados dispendiosa, tempo de inatividade operacional, sanções financeiras e danos à reputação.

Os principais **benefícios** que as empresas que investem na criação de um DRP sólido podem usufruir são os seguintes:

- **Tempo de Inatividade Mais Curto** - muitas das empresas dependem fortemente da tecnologia para as suas operações normais, então, quando um incidente acontece, pode ter consequências graves. Os planos de recuperação de desastres, quando são sólidos e testados rigorosamente, ajudam as empresas a voltar a funcionar o mais rapidamente possível após um incidente;

- **Custos de Recuperação Reduzidos** - a recuperação de um incidente pode ser dispendiosa. De acordo com um relatório da IBM [50], o custo médio de uma falha em 2023 foi de cerca de quatro milhões de dólares, um aumento de 15 % face aos três anos anteriores. As empresas com DRPs podem reduzir significativamente os custos de recuperação do negócio e outras consequências de um incidente não planeado.

9.2. 5 Passos para Construir um Plano de Recuperação de Desastres

O desenvolvimento de um Plano de Recuperação de Desastres começa com uma análise dos processos empresariais, uma análise de risco e alguns objetivos de recuperação claramente definidos.

Embora não exista um modelo único, existem vários passos que as entidades ou empresas podem seguir - independentemente da sua dimensão - para garantir que tem um processo implementado para enfrentar vários incidentes.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

Passo 1 - Efetuar uma análise do impacto comercial

Uma análise do impacto comercial (*Business Impact Analysis*, BIA) é uma avaliação cuidadosa de cada ameaça que uma empresa pode enfrentar e quais podem ser as suas ramificações. Uma BIA sólida examina a forma como uma potencial ameaça pode afetar aspetos como as operações diárias, os canais de comunicação e a segurança dos trabalhadores.

Passo 2 - Analisar os Riscos

Diferentes sectores e tipos de empresas enfrentam **diferentes ameaças**, pelo que a análise de riscos é **fundamental** para determinar a forma de responder a cada uma delas. Pode ser avaliado cada risco separadamente, considerando tanto a sua probabilidade como o seu potencial impacto.

Existem dois métodos amplamente utilizados para determinar o risco: análise de risco qualitativa e quantitativa. A análise qualitativa baseia-se na perceção do risco, enquanto a análise quantitativa é efetuada com base em dados verificáveis.

Passo 3 - Criar um Inventário de Ativos

Para recuperar de um incidente cibernético, é importante ter uma imagem completa dos ativos que a empresa possui. Fazer um inventário regular ajuda a identificar *hardware*, *software*, infra-estruturas de IT, dados e outros ativos que são críticos para as operações comerciais. Podem ser utilizar várias etiquetas para classificar os dados, que serão referidas mais à frente no documento.

Passo 4 - Estabelecer Funções e Responsabilidades

A secção de funções e responsabilidades do plano de recuperação de desastres é bastante importante. Caso esta secção não existisse, era difícil de saber o que fazer quando ocorre um incidente não planeado. Embora as funções e responsabilidades reais variem muito, dependendo do tipo de negócio, aqui estão algumas funções e responsabilidades típicas contidas na maioria dos planos de recuperação de desastres:

- Comunicação de incidentes: Deve designar um indivíduo (ou indivíduos) em cada departamento cuja única responsabilidade é comunicar com a equipa de gestão, as partes interessadas e todas as autoridades relevantes quando ocorrem eventos perturbadores.
- Gestão do DRP: Deve ser nomeado um supervisor do DRP para garantir que os membros da equipa executam as tarefas que lhes são atribuídas e que o DRP funciona corretamente.
- Proteção de ativos: Deve atribuir a alguém a tarefa de assegurar e proteger os seus bens mais importantes quando ocorre uma catástrofe e comunicar o seu estado à administração e às partes interessadas.
- Comunicação com terceiros: Uma pessoa deve ser responsável pela coordenação com os fornecedores terceiros que contratou no âmbito do seu plano de recuperação de desastres. Esta pessoa deve fornecer atualizações constantes sobre a evolução do plano de recuperação de desastres a todos os intervenientes relevantes.

Passo 5 - Testar e Aperfeiçoar

Para garantir que o plano de recuperação de desastres se desenrola sem problemas durante um incidente real, é necessário praticá-lo regularmente e atualizá-lo de acordo com as alterações significativas que ocorrerem na empresa. Por exemplo, se a empresa adquirir um novo ativo após a formação do plano de recuperação de desastres, terá de o incorporar no plano para garantir a sua proteção futura.

Este processo de testar e aperfeiçoar o plano de recuperação de desastres pode ser simplificado em três etapas:

1. Criar uma simulação exata: será importante tentar criar um ambiente que seja o mais próximo possível com o cenário real que a empresa poderá enfrentar;

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027
Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

2. Identificar problemas: ao longo do teste, devem ser identificadas falhas e inconsistências no DRP e tentar resolver os problemas identificados na próximo iteração do plano de recuperação de desastres;

3. Testar as cópias de segurança: é também importante testar os procedimentos de restauração de sistemas críticos quando o incidente terminar. Devem ser testados a forma como se ligam as redes, a recuperação de quaisquer dados perdidos e, por fim, retomar as operações normais.

9.3. A gestão de recursos de dados na empresa

Embora o teletrabalho não seja uma prática muito comum em empresas que não se focam na área tecnológica, este modelo de trabalho irá ser cada vez mais comum e mais aceite como uma forma natural de trabalho, mesmo que não seja para todas as áreas de uma empresa. Uma abordagem que é geralmente implementada nestes tipos de casos é expor diretamente alguns serviços ou recursos para que os colaboradores em teletrabalho podem aceder a esses conteúdos. Esta prática é desaconselhada, visto que expõe a empresa a riscos de ataque desnecessários. Uma solução para isto passa pela criação de um sistema de suporte a uma VPN, que permite que todos os utilizadores com acesso possam trabalhar com segurança a partir de outro local. Assim sendo, os colaboradores trabalham como se estivessem fisicamente na empresa.

Como também já foi referido, é bastante importante a **implementação de um sistema de salvaguarda**, que garante a reposição, parcial ou integral, de toda a informação da empresa, caso aconteça alguma catástrofe ou uma falha simples. Uma forma simples de fazer isto poderia ser copiar os dados para discos ou partilhas na rede, em servidores distintos. Porém uma das ameaças que nos últimos anos se tem globalizado, o ***ransomware*** **, veio mostrar uma grande fragilidade nesta abordagem**, fazendo com que estas abordagens de cópias ficassem comprometidas.

A solução para este problema passará por garantir que o armazenamento das cópias de segurança esteja numa outra camada ou numa outra rede distinta, à qual não há acesso de rede direto a partir dos restantes servidores. Existem diversos *softwares* disponíveis que ajudam neste processo.

É de realçar que estas cópias de segurança devem ser facilmente acessíveis, visto que numa situação de urgência devem ser acedidas o mais rapidamente possível e também para que se possam testar com alguma frequência, para garantir a sua integridade e utilidade.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

10. Ativos

Um ativo [51, 52, 53, 54] é algo que tem um valor para a organização, sendo necessário protegê-lo na ótica da mesma. De acordo com a Lei n.º 46/2018 de 13 de agosto (já referida na secção 3.3), que estabelece o Regime Jurídico da Segurança do Ciberespaço (RJSC), relativa a medidas destinadas a garantir um elevado nível comum de segurança dos sistemas de informação e das redes em toda a União Europeia (UE), entende-se por ativo "todo o sistema de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos (aplicações e plataformas de *software*) considerados essenciais, geridos ou detidos pela entidade, que suportam, direta ou indiretamente, um ou mais serviços".

Um sistema de informação compreende não só *hardware* e *software*, podendo os ativos ser (mas não só) das seguintes categorias:

- Tecnológicos (*hardware*, *software*, sistemas e dispositivos de rede);
- Pessoas;
- Informação;
- Ambiente físico e localizações;
- Dependências contratuais internas ou externas ao serviço.

10.1. Níveis de Classificação

De forma a proteger eficazmente a informação manuseada por cada entidade, torna-se necessário definir um conjunto de categorias a utilizar para descrever os dados e quantificar a quantidade de proteção necessária. Com base na literatura existente, foram definidas cinco categorias onde os dados podem ser divididos e classificados:

- Ultrassecreto;
- Restrito/Secreto;
- Confidencial;
- Interno;
- Público.

10.1.1. Público

Informação que pode ser disseminada sem restrições no seu conteúdo, audiência ou altura de publicação. A sua divulgação não viola nenhuma lei relevante (nomeadamente, leis de privacidade).

10.1.2. Interno

Informação que ser disponibilizada apenas a membros da entidade. A informação divulgada neste nível de classificação não deve ser disponibilizada ao público sem uma revisão anterior, evitando quaisquer repercussões.

10.1.3. Confidencial

Informação confidencial e que requer autorização específica para ser consultada e manipulada. A divulgação deste tipo de informação pode causar danos pessoais, disrupções a um subconjunto da entidade, danos em relações comerciais e perda de vantagem competitiva.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

10.1.4. Restrito/Secreto

Informação restrita ou altamente confidencial que requer o maior cuidado na sua manipulação. A divulgação deste tipo de informação pode resultar em violações significativas de privacidade, riscos de segurança a um indivíduo ou grupo de pessoas, perdas financeiras elevadas (multas, términos de relações contratuais) ou ações reivindicatórias.

10.1.5. Ultrassecreto

O nível ultrassecreto engloba as mesmas propriedades do nível imediatamente abaixo (restrito/secreto), sendo a categoria mais elevada de sensibilidade e requer os maiores níveis de proteção e controlo de acesso. Esta categoria é utilizada quando estritamente necessária, uma vez que a divulgação não autorizada de tal informação pode ter consequências extremamente graves, como danos irreparáveis à entidade, ações judiciais ou reivindicatórias, risco de vida e comprometimento significativo da segurança nacional.

10.2. Gestão de Documentação

A gestão de documentação, independentemente do seu conteúdo e classificação, obriga à delineação e cumprimento de determinados princípios e boas práticas, garantindo assim uma boa gestão de documentação, tanto para documentos em formato físico como em formato digital. A correta gestão da documentação não só facilita a recuperação eficiente das informações, como também garante a conformidade com as regulamentações de proteção de dados, como o RGPD.

É fundamental que todos os funcionários, trabalhadores e colaboradores estejam cientes das políticas e procedimentos estabelecidos para assegurar a proteção da informação e minimizar os riscos associados ao manuseamento inadequado dos documentos.

- Documentos **públicos**
  - Formato **Físico**
    1. **Uso e processamento:**
       Sem restrições;
    2. **Armazenamento:**
       Sem restrições;
  - Formato **Digital**
    1. **Uso e processamento:**
       Sem restrições;
    2. **Armazenamento:**
       Sem restrições.
- Documentos **internos**
  - Formato **Físico**
    1. **Uso e processamento:**
       Sem restrições - fora do local de trabalho, devem guardar-se os documentos quando não estão em utilização;
    2. **Armazenamento:**
       Sem restrições;
  - Formato **Digital**
    1. **Uso e processamento:**
       Sem restrições - fora do local de trabalho, devem guardar-se os documentos quando não estão em utilização;
    2. **Armazenamento :**
       Guardar os documentos no computador de trabalho ou em suporte amovível;
       Bloquear acesso ao computador quando não está em utilização.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027
Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

- Documentos **confidenciais**
  - Formato **Físico**
    1. **Uso e processamento:**
       Os documentos não podem ser consultados fora do local de trabalho ou em locais públicos onde existam outros indivíduos ao redor/ com grande afluência de pessoas;
       Os documentos só devem estar abertos ou em utilização enquanto estão a ser trabalhados. Após a sua consulta ou processamento, devem ser armazenados de forma segura;
    2. **Armazenamento:**
       Guardar os documentos em local seguro e preferencialmente fechado, como um arquivo ou pasta fechada;
       Quando transportados, devem ser manuseados com cuidado para não comprometer a informação contida neles;
  - Formato **Digital**
    1. **Uso e processamento:**
       Os documentos não podem ser consultados fora do local de trabalho ou em locais públicos onde existam outros indivíduos ao redor/ com grande afluência de pessoas;
       Os documentos só devem estar abertos ou em utilização enquanto estão a ser trabalhados. Após a sua consulta ou processamento, devem ser armazenados de forma segura;
       Os documentos apenas podem ser acedidos e utilizados por quem tem direito (sejam funcionários ou pessoas terceiras);
       A política de armazenamento seguro deve estar sempre em vigor;
    2. **Armazenamento:**
       Bloquear acesso ao computador quando não está em utilização.
- Documentos **restritos/secretos**
  - Formato **Físico**
    1. **Uso e processamento:**
       Os documentos não podem ser consultados fora do local de trabalho ou em locais públicos onde existam outros indivíduos ao redor/com grande afluência de pessoas.
       Os documentos só devem estar abertos ou em utilização enquanto estão a ser trabalhados. Após a sua consulta ou processamento, devem ser armazenados de forma segura.
    2. **Armazenamento:**
       Guardar os documentos em local seguro e fechado, como um arquivo ou pasta fechada.
       Quando transportados, devem ser manuseados com cuidado para não comprometer a informação contida neles.
  - Formato **Digital**
    1. **Uso e processamento:**
       Os documentos não podem ser consultados fora do local de trabalho ou em locais públicos onde existam outros indivíduos ao redor/com grande afluência de pessoas.
       Os documentos só devem estar abertos ou em utilização enquanto estão a ser trabalhados. Após a sua consulta ou processamento, devem ser armazenados de forma segura.
       Os documentos apenas podem ser acedidos e utilizados por quem tem direito (sejam funcionários ou pessoas terceiras).
       A política de armazenamento seguro deve estar sempre em vigor;

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

2. **Armazenamento:**
   Bloquear acesso ao computador quando não está em utilização.

- Documentos **ultrassecretos**
  - Formato **Físico**
    1. **Uso e processamento:**
       Os documentos não podem ser consultados fora do local de trabalho ou em locais públicos onde existam outros indivíduos ao redor/com grande afluência de pessoas.
       Os documentos só devem estar abertos ou em utilização enquanto estão a ser trabalhados. Após a sua consulta ou processamento, devem ser armazenados de forma segura.
    2. **Armazenamento:**
       Guardar os documentos em local seguro e fechado, como um arquivo ou pasta fechada.
       Quando transportados, devem ser manuseados com cuidado para não comprometer a informação contida neles.
  - Formato **Digital**
    1. **Uso e processamento:**
       Os documentos não podem ser consultados fora do local de trabalho ou em locais públicos onde existam outros indivíduos ao redor/com grande afluência de pessoas.
       Os documentos só devem estar abertos ou em utilização enquanto estão a ser trabalhados. Após a sua consulta ou processamento, devem ser armazenados de forma segura.
       Os documentos apenas podem ser acedidos e utilizados por quem tem direito (sejam funcionários ou pessoas terceiras).
       A política de armazenamento seguro deve estar sempre em vigor;
    2. **Armazenamento:**
       Bloquear acesso ao computador quando não está em utilização.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027
Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

11. Gestão e Práticas de E-mail

11.1. Gestão do Correio Eletrónico

A **gestão de correio eletrónico** [55, 56, 57] refere-se à prática de **organizar, estabelecer prioridades e tratar os e-mails** de forma a otimizar a produtividade e a eficiência. Envolve estratégias para gerir os e-mails recebidos, responder prontamente e organizar os arquivos de e-mail para facilitar a sua recuperação. Algumas táticas e estratégias comprovadas de gestão de correio eletrónico são as seguintes:

- **Atribuir tempo para o correio eletrónico**

Tal como se reserva tempo para outras tarefas, deve fazer-se o mesmo com o e-mail. É importante fazer isso para não se verificar o correio eletrónico constantemente. A estratégia fundamental para resolver isto é reservar um tempo fixo todos os dias para lidar com o correio eletrónico. Isto pode ser feito apenas uma vez ao dia, mas será mais inteligente programar blocos de tempo ao longo do dia para o correio eletrónico. Também se deve evitar realizar outras tarefas aquando a verificação do e-mail, para minimizar as distrações.

- **Criar etiquetas, pastas e categorias**

Uma forma de simplificar o manuseamento do correio eletrónico é através da organização, o que envolve a criação de etiquetas, pastas e categorias. Não existe uma regra sobre como esta organização deve ser feita, esta apenas tem de se adequar o melhor possível a cada pessoa. A chave é priorizar, agrupar e classificar os e-mails em categorias. A maior vantagem deste ponto é que se torna mais fácil de localizar e-mails mais específicos com apenas alguns cliques.

- **“Tocar uma vez”**

O princípio de “tocar uma vez” ou *touch-it-once* é baseado na tomada de decisões rápidas no tratamento de mensagens de correio eletrónico. A ideia por trás deste método é que revisitar o mesmo e-mail várias vezes é uma perda de tempo. A ideia é que se toque apenas uma vez em cada e-mail, tomando-se as medidas adequadas para esse e-mail (podendo também basear-se nos 4 D’s). Apesar do conceito ser fácil de entender, pode ser difícil de seguir quando se trata de correio eletrónico, porque temos a tendência a adiar a resposta aos e-mails. Mas adotar esta estratégia é importante, e pode aumentar a produtividade.

- **Regra do um minuto**

Esta regra tem um conceito simples atrás dela: se demora apenas um minuto a responder a um e-mail, faça-o imediatamente. Desta forma, o e-mail fica logo respondido e pode também logo ser arquivado, limpando a caixa de entrada mais rapidamente.

- **Ler de cima para baixo, escrever de baixo para cima**

Atish Davda, o diretor executivo da EquityZen, propõe uma forma única de passar pela caixa de entrada do correio eletrónico. A ideia é ler os e-mails em ordem cronológica inversa e responder aos mesmos por ordem cronológica. Citando Atish, “Este truque tem em conta o facto de algumas pessoas responderem aos e-mails imediatamente, o que por vezes desencadeia um ”jogo de ténis”de e-mails, consumindo aquela hora que reservou para tratar de toda a sua caixa de entrada e deixando-o para trás. Se responder aos e-mails por ordem cronológica, é menos provável que seja apanhado em e-mails de ida e volta e mais provável que se mantenha no caminho certo.”.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

- **Saber quando enviar e-mails**

Saber gerir o correio eletrónico tem tanto a ver com o tipo e volume de correio eletrónico que se recebe, mas também com o que se envia. Uma das formas de enviar menos e-mails é escolher que conversas se devem ter por e-mail e que conversas se devem ter por telefone. Se for necessário apenas dar uma informação simples, uma atualização, o correio eletrónico funciona. Mas se for necessário dar informações mais complexas, talvez a comunicação via telefone seja mais fácil, porque se o assunto for tratado via e-mail pode gerar muitas idas e vindas dos mesmos.

- **Converter as contas de correio eletrónico de grupo em caixas de entrada partilhadas**

A maioria das empresas tem contas de correio eletrónico de grupo, o que facilita o contacto das pessoas externas com a sua marca. Mas esta solução pode não ser a mais ideal. Há um grande fluxo de e-mails recebidos nessas contas, que é agravado pelo facto de não existir uma forma fácil de atribuir mensagens de correio eletrónico a indivíduos e de manter o controlo dessas tarefas. É necessário organizar os e-mails recebidos de modo a que cada membro da equipa saiba claramente o que tem de fazer.

Uma das formas que também é usada para a gestão do correio eletrónico é o uso de *software* para esse fim. Um *software* de gestão de correio eletrónico é uma ferramenta que ajuda os utilizadores a gerir, priorizar, enviar, acompanhar e organizar e-mails. Este tipo de *software* compreende uma variedade de soluções que podem ser utilizadas tanto por indivíduos como por empresas.

Estas são apenas algumas dicas, as mais essenciais para uma melhor gestão do correio eletrónico. Para além destas recomendações, há uma mnemónica (que vem do Inglês) que se pode associar à gestão do correio eletrónico, os 4 D's.

Os 4 D's da gestão de correio eletrónico são os seguintes:

- **Eliminar**(*delete*) – eliminar imediatamente as mensagens de correio eletrónico irrelevantes ou sem importância;
- **Delegar**(*delegate*) – atribuir à pessoa adequada as mensagens de correio eletrónico que podem ser tratadas por outra pessoa;
- **Fazer**(*do*) – responder às mensagens de correio eletrónico que requerem ação imediata;
- **Adiar**(*defer*) – adiar o tratamento de mensagens de correio eletrónico que requerem mais tempo ou consideração para uma altura posterior.

Resumindo, para uma melhor gestão do correio eletrónico, devem ser seguidas as dicas anteriormente apresentadas, ou seja, verificar o correio eletrónico em horas específicas do dia, usar o método dos 4 D's para processar rapidamente e priorizar os e-mails recebidos, utilizar ferramentas ou software de gestão de correio eletrónico para automatizar tarefas repetitivas e organizar a caixa de entrada, considerar a possibilidade de agrupar tarefas semelhantes para aumentar a eficiência e concentrar-se em tratar primeiro os e-mails de alta prioridade e adiar os menos urgentes para mais tarde.

11.2. Proteção contra *Phishing*

Phishing é um **ataque** que tenta roubar dados, informações, dinheiro ou a identidade de alguém, levando essa pessoa a revelar informações pessoais (números de cartões de crédito, informações bancários, palavras-passe, entre outros) através de sites ou e-mails que parecem legítimos. Normalmente, os ciber-criminosos fazem-se passar por empresas numa mensagem **falsa** que contém alguma ligação suspeita.

Como reconhecer uma mensagem ou e-mail de *phishing*?

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

O *phishing* é uma forma popular de cibercrime devido à sua eficácia. As técnicas de *phishing* têm sido cada vez mais sofisticadas, e por isso é preciso estar bastante atento aos e-mails que se recebem. A melhor defesa é a consciencialização e saber o que procurar.

Algumas formas de reconhecer um e-mail de *phishing* são as seguintes:

- **Apelos urgentes à ação ou ameaças -** e-mails ou mensagens que afirmem que tem de clicar ou abrir um anexo imediatamente devem deixá-lo desconfiado. Criar um falso sentido de urgência é um truque comum dos ataques de *phishing* e das burlas;

> **Dica**
> Sempre que vir uma mensagem a apelar a ação imediata, deve parar um momento e analisar **cuidadosamente** a mensagem. Tem a certeza de que a mesma é verdadeira? Seja cauteloso e esteja seguro.

- **Remetentes -** embora não seja invulgar receber mensagens de correio eletrónico pela primeira vez, especialmente se a pessoa não pertencer à sua organização, mas isto poderá ser um sinal de *phishing*. Tenha mais cuidado nessas alturas. Quando receber um e-mail de alguém que não reconheça, pare um momento para o examinar com mais cuidado;
- **Ortografia e gramática incorreta -** se uma mensagem de correio eletrónico tiver erros ortográficos ou gramaticais óbvios, pode tratar-se de uma burla. Esses erros são, geralmente, o resultado de uma tradução incorreta a partir de uma língua estrangeira, e, por vezes, são deliberados numa tentativa de contornar os filtros que tentam bloquear estes ataques;
- **Saudações genéricas -** se o e-mail começar com um genérico "Caro senhor ou senhora", é um sinal de aviso de que pode não ser realmente o seu banco ou site de compras;
- **Domínios de correio eletrónico incompatíveis -** se o e-mail afirmar ser de uma empresa respeitável, como a Microsoft ou o seu banco, mas se o correio eletrónico estiver a ser enviado a partir de outro domínio, é provável que seja burla. Esteja atento a erros ortográficos subtis no nome do domínio, visto que este é um truque bastante comum;
- **Hiperligações ou Anexos Suspeitos -** se suspeitar que uma mensagem de correio eletrónico possa ser de *phishing*, **não abra nenhuma hiperligação** (*links*) **nem anexos** que possam estar no e-mail.

Apesar destas técnicas serem bastante comuns nos e-mails de *phishing*, tenha sempre atenção a outros sinais que possam ser duvidosos. Como já foi referido em cima, as técnicas de *phishing* estão cada vez mais evoluídas e mais sofisticadas, pelo que **todo o cuidado é pouco**.

11.3. Outras práticas

A utilização de endereços institucionais personalizados para a empresa, nas contas que gerem ou transacionam informação **é uma prática a adotar**. Além de uma maior credibilidade, ajuda os restantes parceiros e também os clientes a identificarem melhor caso haja alguma tentativa de impersonificação em nome da empresa.

Uma medida adicional neste contexto é inserir nos e-mails **assinaturas digitais qualificadas**, como constam no cartão de cidadão, visto que estas assinaturas permitem validar, de forma inequívoca, o remetente.

No cumprimento das regras definidas pelo RGPD, os colaboradores de um empresa com endereço de e-mail "pessoal"no domínio da empresa, impede que este seja consultado por outra pessoa. Esta limitação impede que o endereço de e-mail não possa ser consultado (e por isso utilizado) por outro membro da empresa. É assim recomendado que os endereços relativos a áreas ou serviços da empresa sejam criados de forma despersonalizada, sem mencionar nomes de pessoas que possam gerir esse endereço de e-mail.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

12. Uso de Servidores

Um **servidor** é um dispositivo de *hardware* que processa os pedidos enviados através de uma rede e responde aos mesmos. Um **cliente** é um dispositivo que submete um pedido e aguarda uma resposta do servidor. A arquitetura do servidor é chamada de **modelo cliente-servidor**.

Os servidores [58, 59, 60] desempenham uma função importante em qualquer rede. Frequentemente, um servidor é um computador de alto desempenho que utiliza software especializado ou sistemas operativos para armazenar dados e centralizar recursos num escritório ou empresa.

O papel dos servidores tem-se tornado cada vez mais essencial. Quer se trate de uma pequena empresa ou de uma empresa já estabelecida, investir num servidor pode trazer benefícios significativos que vão para além do mero armazenamento de dados. Algumas das vantagens do uso de servidores são as seguintes:

- Gestão centralizada de dados: um servidor funciona como um *hub* centralizado para armazenar e gerir os dados da empresa, significando que os dados estão armazenados num local, que simplifica o acesso e facilita a gestão dos dados;
- Segurança reforçada: as empresas lidam com dados sensíveis, o que faz com que a segurança seja uma prioridade. Um servidor fornece funcionalidades de segurança, incluindo *firewalls*, encriptação e autenticação do utilizador, o que protege os dados contra o acesso não autorizado;
- Colaboração melhorada: com capacidades centralizadas de armazenamento e partilha de ficheiros, os funcionários de uma empresa podem colaborar e trabalhar simultaneamente em projetos e aceder a documentos partilhados de forma eficaz;
- Cópia de segurança confiável dos dados: a perda de dados pode ter consequências desastrosas para uma empresa. Um servidor oferece soluções de cópias de segurança robustas, garantindo que os dados de uma empresa são regularmente guardados e podem ser facilmente restaurados em caso de algum incidente;
- Escalabilidade: um servidor proporciona escalabilidade, o que permite expandir a infraestrutura e acomodar as necessidades crescentes de uma empresa sem que o desempenho seja comprometido;
- Acesso remoto e mobilidade: numa era em que o trabalho remoto é cada vez mais frequente, um servidor permite que se possa aceder remotamente a recursos empresariais.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

13. Gestão de contas de um *Active Directory*

O ***Active Directory (AD)*** [61, 62, 63, 64, 65, 66, 67, 68] é uma **implementação de serviço de diretório** que armazena informações acerca de objetos em redes de computadores e **disponibiliza** essas informações aos utilizadores e administradores da rede. É um *software* da Microsoft utilizado em ambientes Windows.

Um *Active Directory* armazena informações sobre objetos na rede e torna essas informações fáceis de encontrar e utilizar pelos administradores e pelos utilizadores. O *Active Directory* utiliza armazenamento de dados estruturado como base para uma organização lógica e hierárquica das informações da diretoria.

A segurança está integrada no *Active Directory* através da **autenticação de inícios de sessão** e **controlo de acesso** a objetos na diretoria. Os administradores podem gerir os dados e a organização do Directory em toda a rede, e os utilizadores autorizados da rede podem aceder a recursos em qualquer ponto da rede.

O *Active Directory* inclui também:

- Um **conjunto de regras**, ou esquema, que define as classes dos objetos e atributos contidos na diretoria, as restrições e limites das instâncias desses objetos e o formato dos seus nomes;
- Um **catálogo** que contém informações sobre todos os objetos que estão no Active Directory. Isto permite que os utilizadores e administrados encontrem informações sobre a diretoria, independentemente do domínio em que realmente se encontram os dados;
- Um **mecanismo de consulta e índice**, para que os objetos e as suas propriedades possam ser publicados e encontrados facilmente pelos utilizadores ou aplicações da rede;
- Um Business Continuity Plan que distribui os dados da diretoria por uma rede. Todos os controladores de domínio participam na replicação e contêm uma cópia completa de todas as informações da diretoria do respetivo domínio. Qualquer alteração aos dados da diretoria é replicada para todos os controladores de domínio no domínio.

A estrutura do *Active Directory* incorpora os seguintes componentes:

- **Computadores e utilizadores** - auto-explicativo. Cada conta é descrita por atributos como o nome, cargo, endereço de email, entre outros;
- **Unidades organizacionais** - elementos que organizam os utilizadores, grupos, computadores e outros recursos;
- **Domínios** - coleção de objetos agrupada dentro de uma rede cliente-servidor e autenticada num único banco de dados;
- **Árvores** - uma árvore de domínios é composta por vários domínios que compartilham um esquema ou configuração comum;
- **Floresta** - extensão hierárquica de uma árvore. É um limite administrativo que serve para facilitar a gestão e autenticação de várias árvores, domínios e objetos.

13.1. Terminologia (ou relações) de confiança

O *Active Directory* depende de relações de confiança para moderar os direitos de acesso a recursos entre domínios. Existem diferentes tipos de relações de confiança, que serão apresentadas de seguida.

A **confiança unidirecional** ocorre quando um primeiro domínio permite privilégios de acesso a utilizadores num segundo domínio, no entanto o segundo domínio não permite o acesso aos utilizadores do primeiro domínio. Já uma **confiança bidirecional** ocorre quando existem dois domínios e estes permitem o acesso de ambos. Uma **confiança externa** é uma

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

confiança que liga domínios em florestas separadas ou domínios que não são AD. Estas ligações podem ser não transitivas, unidirecionais ou bidirecionais.

Uma **confiança de gestão de acesso privado** (PAM) é uma confiança unidirecional criada pelo *Microsoft Identity Manager* entre uma floresta de produção e uma floresta de bastião.

Um **domínio de confiança** é um domínio único que permite o acesso do utilizador a outro domínio.

Uma **ligação de confiança transitiva** pode estender-se para além de dois domínios e permitir o acesso a outros domínios de confiança numa floresta. Uma **ligação de confiança intransitiva** é uma confiança unidirecional que se limita a dois domínios.

Uma **confiança explícita** é uma confiança unidirecional e não transitiva que é criada por um administrador de rede. Uma **confiança de ligação cruzada** é um tipo de confiança explícita. Este tipo de relação de confiança ocorre entre domínios dentro de (1) a mesma árvore, sem relação pai-filho entre os dois domínios, ou (2) árvores diferentes. Uma **confiança de floresta** aplica-se a domínios dentro de toda a floresta e pode ser unidirecional, bidirecional ou transitiva.

Um **atalho** junta dois domínios que pertencem a árvores separadas. Estes podem ser unidirecionais, bidirecionais ou transitivos.

Um **domínio** é uma confiança que é transitiva, intransitiva, unidirecional ou bidirecional.

13.2. Benefícios do uso de um *Active Directory*

O AD fornece mais do que apenas um serviço unificado; é um ativo inestimável para as organizações que pretendem simplificar as suas operações de IT e reforçar a sua segurança. As vantagens principais de um AD são as seguintes:

- **Gestão centralizada de recursos:**
  - **Partilha simplificada de recursos** - O Active Directory permite aos administradores de IT gerirem recursos de rede (utilizadores, computadores, ficheiros partilhados, impressoras) a partir de um ponto central, o que simplifica a gestão dos recursos;
  - **Gestão de utilizadores simplificada** - o AD simplifica a gestão de contas de utilizadores ao fornecer uma plataforma centralizada para criar, modificar ou eliminar utilizadores em toda a rede;
- **Segurança melhorada:**
  As funcionalidades de segurança robustas do AD protegem os dados sensíveis contra ameaças cibernéticas. As políticas de grupo e os controlos de acesso impõem requisitos de palavras-passe rigorosas e limitam o acesso dos utilizadores a ficheiros ou aplicações específicos com base nas suas funções específicas na empresa;
- **Escalabilidade e flexibilidade:**
  - **Arquitetura escalável** - o AD pode gerir pequenas redes, assim como ambientes empresariais grandes e complexos, o que o torna flexível para organizações de diferentes dimensões;
  - **Vários domínios e florestas** - os *Active Directories* suportam a criação de vários domínios, florestas e unidades organizacionais, o que proporciona flexibilidade na gestão de diferentes partes de uma organização de forma independente, e mantendo o controlo centralizado;
- **Controlo de acesso baseado em funções:**
  Os administradores podem definir permissões de acesso com base em funções de utilizador, grupos ou critérios específicos. Isto garante que os utilizadores apenas têm acesso aos recursos que necessitam com base nas suas funções, minimizando assim o risco de acesso não autorizado;

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

- **Resolução de problemas mais rápida:**
  Ter um sistema centralizado como o *Active Directory* ajuda a diagnosticar mais rapidamente qualquer problema que possa surgir, fornecendo registos detalhados sobre as atividades dos utilizadores e os eventos do sistema.

13.3. Contas do *Active Directory*

Existem diversos tipos de contas que servem diferentes objetivos num *Active Directory*. Segue-se uma análise dos tipos principais:

1. **Contas de Utilizador**
   - **Conta de Utilizador *Standard*** - contas criadas para utilizadores individuais para permitir o acesso aos recursos da rede. Normalmente, cada utilizador tem um nome de utilizador e uma palavra-passe únicos. As permissões são atribuídas com base nas necessidades do utilizador;
   - **Conta de Administrador** - esta é uma conta de utilizador especial com permissões elevadas, frequentemente utilizada para gerir a infraestrutura do AD. Os administradores podem criar, eliminar e gerir outras contas e recursos no AD;
   - **Conta de Convidado** - normalmente desativada por predefinição, a conta de convidado destina-se ao acesso temporário ou limitado de utilizadores que não têm uma conta dedicada no domínio.
2. **Contas de Computador**
   - **Contas de computador ligadas ao domínio** - criadas quando um computador se junta ao domínio, estas contas representam dispositivos como estações de trabalho e servidores. Ajudam a autenticar e gerir dispositivos na rede;
   - **Contas de controlador de domínio** - estas são contas de computador especializadas que representam controladores de domínio, que são servidores críticos que alojam os serviços do *Active Directory*.
3. **Contas de Serviço**
   - **Conta de serviço local** - esta conta tem permissões limitadas e é utilizada para executar serviços localmente num computador, principalmente em controladores que não sejam de domínio;
   - **Conta de serviço de rede** - semelhante à anterior, mas com permissões adicionais para aceder a recursos de rede, é utilizada para serviços que necessitam de se ligar através da rede;
   - **Conta de Serviço Gerido** - as contas de serviço geridas são concebidas para executar serviços com gestão automática de palavras-passe. São frequentemente utilizadas para executar serviços em servidores individuais;
   - **Conta de Serviço Gerido por Grupo** - uma conta deste tipo pode ser utilizada em vários servidores, permitindo uma conta de serviço partilhada com gestão automática de palavras-passe, o que é vantajoso para serviços de alta disponibilidade ou quintas de servidores.
4. **Contas de grupo**
   - **Grupos de segurança** - utilizados para gerir as permissões dos recursos no domínio. Os grupos de segurança são normalmente utilizados para atribuir permissões de controlo de acesso a ficheiros, pastas e outros recursos;
   - **Grupos de distribuição** - são utilizados principalmente para listas de distribuição de correio eletrónico em ambientes Microsoft Exchange e não têm permissões de segurança associadas por predefinição.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027
Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

5. **Contas incorporadas**
    - **Conta de administrador padrão** - uma conta altamente privilegiada criada por defeito em todos os ambientes AD, frequentemente utilizada para a instalação e configuração iniciais.
    - **Conta de sistema local** - uma conta de sistema poderosa que pode aceder a praticamente todos os recursos do sistema; utilizada principalmente pelo sistema operativo e por alguns serviços críticos.
    - **Conta KRBTGT** - esta é uma conta de sistema utilizada pelo Centro de Distribuição de Chaves Kerberos (KDC) para atribuição de bilhetes em ambientes AD. É essencial para a autenticação Kerberos e é criada automaticamente durante a configuração do AD;
6. **Contas de aplicação** - são contas de serviço ou de utilizador criadas especificamente para as aplicações acederem aos recursos da rede. Muitas vezes, requerem permissões específicas para interagir com objetos do AD e podem ser configuradas como contas de serviço gerido ou de serviço gerido por grupos, para simplificar a gestão de credenciais.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

14. Outras recomendações

Em forma de conclusão, este capítulo apresenta um resumo das recomendações feitas ao longo deste guia. A lista [69] abaixo apresenta então os vários pontos:

- Manter sempre os sistemas operativos e softwares atualizados regularmente, aplicando patches e atualizações de segurança fornecidos pelo fabricante;
- Utilizar antivírus e *firewalls* em todos os dispositivos, incluindo computadores fixos, portáteis, *smartphones* e *tablets*;
- Abrir apenas emails de remetentes que conhece (pelo endereço e não pelo nome), e reportando quaisquer emails suspeitos, em especial aqueles com *links* ou anexos dúbios ou não solicitados;
- Ativar o bloqueio automático de dispositivos, nunca os deixando desbloqueados por longos períodos ou de ausência prolongada;
- Utilizar passwords com mais de 12 caracteres, com maiúsculas, minúsculas, algarismos e caracteres especiais;
- Alterar regularmente as passwords e não reutilizar as mesmas em sítios diferentes;
- Utilizar a VPN da organização em redes públicas ou fora do local habitual de trabalho;
- Ativar a autenticação de dois fatores (2FA) sempre que possível;
- Manter cópias de segurança (backups) armazenados em locais seguros e protegidos contra acessos não autorizados;
- Ativar a encriptação de disco em computadores e dispositivos amovíveis, como pen drives, discos externos ou cartões de memória;
- Anonimizar, ou disponibilizar informação pessoal estritamente necessária nos vários serviços online, como redes sociais, plataformas ou sítios web;
- Verificar as definições e permissões de acessos das várias aplicações, seja no computador ou no telemóvel, em intervalos regulares (por exemplo, trimestralmente);
- Não instalar software de origem desconhecida ou questionável;
- Cobrir ou desativar webcams e microfones, ativando-os apenas quando necessário;
- Certificar-se da utilização do protocolo HTTPS ao navegar na Internet, especialmente em websites onde se introduzam credenciais ou informação pessoal, como o acesso ao homebanking, ao email e serviços de saúde;
- Reportar e eliminar mensagens de tentativa de phishing ou exfiltração de credenciais;
- Manter uma atitude de espírito crítico e bom-senso informático;
- Em caso de dúvida, contactar o suporte informático da empresa ou serviço em questão, solicitando informações adicionais para cada dúvida.

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

Referencias

[1] A. W. Services. O que é o modelo OSI? [Online]. Available: https://aws.amazon.com/pt/what-is/osi-model/

[2] Cloudflare. What is the OSI Model? [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

[3] ——. What is the OSI Model? [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

[4] ——. O que é um protocolo? | Definição de protocolo de rede. [Online]. Available: https://www.cloudflare.com/pt-br/learning/network-layer/what-is-a-protocol/

[5] ——. What is HTTP? [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/

[6] ——. What is the Simple Mail Transfer Protocol (SMTP)? [Online]. Available: https://www.cloudflare.com/learning/email-security/what-is-smtp/

[7] ——. What is the Internet Protocol? [Online]. Available: https://www.cloudflare.com/learning/network-layer/internet-protocol/

[8] ——. What is TCP/IP? [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/tcp-ip/

[9] ——. What is UDP? [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/user-datagram-protocol-udp/

[10] Clouflare. What is the Internet Control Message Protocol (ICMP)? [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/internet-control-message-protocol-icmp/

[11] Cloudflare. What is IGMP? | Internet Group Management Protocol. [Online]. Available: https://www.cloudflare.com/learning/network-layer/what-is-igmp/

[12] ——. What is IPsec? | How IPsec VPNs work. [Online]. Available: https://www.cloudflare.com/learning/network-layer/what-is-ipsec/

[13] INCIBE. Instituto Nacional de Ciberseguridad. [Online]. Available: https://www.incibe.es/en

[14] D. da República. Lei n.º 46/2018, de 13 de agosto. [Online]. Available: https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384

[15] CNCS. Regime Jurídico. [Online]. Available: https://www.cncs.gov.pt/pt/regime-juridico/

[16] WeSecure. REGIME JURÍDICO DA SEGURANÇA DO CIBERESPAÇO (DL 65/2021). [Online]. Available: https://www.wesecure.pt/regime_juridico_da_seguranca_do_ciberespaco_dl_65_2021/

[17] IGFEJ. Regulamento Geral de Proteção de Dados (RGPD). [Online]. Available: https://igfej.justica.gov.pt/Sobre-o-IGFEJ/Regulamento-Geral-de-Protecao-de-Dados-RGPD

[18] EUR-Lex. Regulamento Geral sobre a Proteção de Dados (RGPD). [Online]. Available: https://eur-lex.europa.eu/PT/legal-content/summary/general-data-protection-regulation-gdpr.html

[19] CNCS. Diretiva SRI 2 (NIS 2). [Online]. Available: https://www.cncs.gov.pt/pt/diretiva-sri-2-nis-2/#collapse1Two

[20] TechTarget. 5 Reasons Software Updates are Important. [Online]. Available: https://www.techtarget.com/whatis/feature/5-reasons-software-updates-are-important

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

[21] Medium. The Importance of Regular Software Updates And Patches. [Online]. Available: https://medium.com/@findmyservices/the-importance-of-regular-software-updates-and-patches-c2f362cef981

[22] pplware. 5 razões para manter os seus dispositivos e software atualizados. [Online]. Available: https://pplware.sapo.pt/internet/5-razoes-para-manter-os-seus-dispositivos-e-software-atualizados/

[23] LinkedIn. POR QUE A ATUALIZAÇÃO REGULAR DE SOFTWARES É IMPORTANTE? [Online]. Available: https://www.linkedin.com/pulse/por-que-atualiza%C3%A7%C3%A3o-regular-de-softwares-%C3%A9-importante-gofix/

[24] U. of Idaho. Why keeping your software up to date is important for cybersecurity? [Online]. Available: https://support.uidaho.edu/TDClient/40/Portal/KB/ArticleDet?ID=2770

[25] W. University. Cybersecurity 101: Why Choosing a Secure Password Is So Important. [Online]. Available: https://www.waldenu.edu/programs/information-technology/resource/cybersecurity-101-why-choosing-a-secure-password-in-so-important

[26] C. N. de Cibersegurança. Boas práticas no uso de palavras-passe. [Online]. Available: https://www.cncs.gov.pt/pt/boas-praticas-passwords/

[27] Microsoft. What is access control? [Online]. Available: https://www.microsoft.com/en-us/security/business/security-101/what-is-access-control

[28] Citrix. What is access control? [Online]. Available: https://www.citrix.com/glossary/what-is-access-control.html

[29] Medium. Autenticação, controle de acesso e Análise de vulnerabilidade. [Online]. Available: https://medium.com/@celionormando/autentica%C3%A7%C3%A3o-e-controle-de-acesso-e-an%C3%A1lise-de-vulnerabilidade-f68726d203c2

[30] Cisco. What Is Network Monitoring? [Online]. Available: https://www.cisco.com/c/en/us/solutions/automation/what-is-network-monitoring.html

[31] M. Engine. Basics of Network Monitoring. [Online]. Available: https://www.manageengine.com/network-monitoring/basics-of-network-monitoring.html

[32] NordLayer. The comprehensive guide to network security monitoring. [Online]. Available: https://nordlayer.com/blog/the-guide-to-network-security-monitoring/

[33] G. for Geeks. Intrusion Detection System (IDS). [Online]. Available: https://www.geeksforgeeks.org/intrusion-detection-system-ids/

[34] IBM. What is an intrusion detection system (IDS)? [Online]. Available: https://www.ibm.com/topics/intrusion-detection-system

[35] G. for Geeks. Intrusion Prevention System (IPS). [Online]. Available: https://www.geeksforgeeks.org/intrusion-prevention-system-ips/

[36] IBM. What is an intrusion prevention system (IPS)? [Online]. Available: https://www.ibm.com/topics/intrusion-prevention-system

[37] ——. What is endpoint detection and response (EDR)? [Online]. Available: https://www.ibm.com/topics/edr

[38] Cisco. What Is Endpoint Detection and Response (EDR)? [Online]. Available: https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr-medr.html

[39] Microsoft. O que é a EDR (detecção e resposta de ponto de extremidade)? [Online]. Available: https://www.microsoft.com/pt-br/security/business/security-101/what-is-edr-endpoint-detection-response

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027
Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

[40] IBM. What is security information and event management (SIEM)? . [Online]. Available: https://www.ibm.com/topics/siem

[41] Microsft. What is SIEM? [Online]. Available: https://www.microsoft.com/en-us/security/business/security-101/what-is-siem

[42] Cohesity. Data backup and recovery. [Online]. Available: https://www.cohesity.com/glossary/backup-and-recovery/

[43] A. W. Services. O que é backup de dados? [Online]. Available: https://aws.amazon.com/pt/what-is/data-backup/

[44] Veritas. Backup e recuperação de dados: o guia essencial. [Online]. Available: https://www.veritas.com/pt/br/information-center/data-backup-and-recovery

[45] IBM. O que é backup e restauração? [Online]. Available: https://www.ibm.com/br-pt/topics/backup-and-restore

[46] Lenovo. What is backup? [Online]. Available: https://www.lenovo.com/us/en/glossary/backup/

[47] Veritas. Regra de backup 3 2 1: garantindo a proteção e recuperação de dados. [Online]. Available: https://www.veritas.com/pt/br/information-center/3-2-1-backup-rule

[48] IBM. What is a disaster recovery plan (DRP)? [Online]. Available: https://www.ibm.com/topics/disaster-recovery-plan

[49] G. Cloud. O que é um plano de recuperação de desastres? [Online]. Available: https://cloud.google.com/learn/what-is-disaster-recovery?hl=pt-BR

[50] IBM. Cost of a Data Breach Report 2024. [Online]. Available: https://www.ibm.com/reports/data-breach

[51] B. U. Policies. Data Classification Policy. [Online]. Available: https://www.bu.edu/policies/data-classification-policy/

[52] R. Portuguesa. Informação Classificada. [Online]. Available: https://www.gns.gov.pt/docs/questes-sobre-informao-classificada.pdf

[53] U. of Hong Kong. Information Security and Data Management Policy. [Online]. Available: https://isdm.hku.hk/

[54] U. of Arkansas. Data Lifecycle and Management Policy/Procedures. [Online]. Available: https://uada.edu/docs/policies/UADA_920_1.pdf

[55] R. Content. 7 Best Practices and Tips to Effective Email Management. [Online]. Available: https://rockcontent.com/blog/email-management/

[56] Hiver. 23 Email Management Best Practices and Tips. [Online]. Available: https://hiverhq.com/blog/email-management

[57] ZenDesk. Best 13 email management software of 2024. [Online]. Available: https://www.zendesk.com/service/ticketing-system/email-management-software/

[58] Medium. 8 Reasons Why Your Business Needs a Server. [Online]. Available: https://medium.com/@EvaAdams1/8-reasons-why-your-business-needs-a-server-a22c9cbb6c7b

[59] ZDNET. 5 Reasons Your Business Needs a Server. [Online]. Available: https://www.zdnet.com/paid-content/article/5-reasons-your-business-needs-a-server/

[60] HP. How to Set Up a Server for Small Business. [Online]. Available: https://www.hp.com/us-en/shop/tech-takes/how-to-set-up-server-for-small-business

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.

[61] Microsoft. Active Directory accounts. [Online]. Available: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-default-user-accounts

[62] Rockspace. Create, manage, and delete users and groups in Active Directory. [Online]. Available: https://docs.rackspace.com/docs/create-manage-and-delete-users-and-groups-in-active-directory

[63] S. Space. How to Manage User Accounts in Active Directory. Part 1: Creating and Deleting User Accounts. [Online]. Available: https://serverspace.io/support/help/how-to-manage-user-accounts-in-active-directory-part-1-creating-and-deleting-user-accounts/

[64] Wikipedia. Active Directory. [Online]. Available: https://en.wikipedia.org/wiki/Active_Directory

[65] Microsoft. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview. [Online]. Available: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

[66] Quest. What is Active Directory and how does it work? [Online]. Available: https://www.quest.com/solutions/active-directory/what-is-active-directory.aspx

[67] TechTarget. What is Active Directory and how does it work? [Online]. Available: https://www.techtarget.com/searchwindowsserver/definition/Active-Directory

[68] proofpoint. What Is Active Directory? [Online]. Available: https://www.proofpoint.com/us/threat-reference/active-directory

[69] CNCS. Boas Práticas de Cibersegurança. [Online]. Available: https://www.cncs.gov.pt/docs/1626335247.pdf

Este proyecto ha sido financiado por el fondo europeo de desarrollo regional (FEDER) en el marco del programa Interreg VI-A España – Portugal POCTEP 2021-2027 Proyecto: CIBERIA - Digitalización y resiliencia transfronteriza mediante el fomento de una zona CENCYL cibersegura (0192_CIBERIA_3_E.