SEGURANÇA DIGITAL

NOS NOVOS NEGÓCIOS

INFORMAÇÃO TÉCNICA FOCADA NAS TENDÊNCIAS EMPRESARIAIS E NA CRIAÇÃO DE NOVAS EMPRESAS DE BASE TECNOLÓGICA

ÍNDICE

ÍNDICE

INTRODUÇÃO

A história mostra que a sociedade vivencia saltos tecnológicos que permitem uma mudança no modo de vida, nomeadamente pela criação de produtos, processos e serviços inovadores. Algumas descobertas alavancaram um rápido desenvolvimento da sociedade: o motor a vapor foi um dos grandes saltos, que permitiu a revolução industrial na Inglaterra do século XVIII e que visava substituir a mão de obra humana por máquinas que executavam as mesmas funções com maior eficiência.

Desde então, novas tecnologias têm vindo a surgir e a fazer parte da alteração do quotidiano da espécie humana. Um novo salto tecnológico foi dado com a descoberta dos semicondutores e da sua evolução, implicando o aparecimento de computadores.

O recurso aos computadores e ao seu poder de computação, é cada vez mais presente nas operações comerciais, industriais e também na vida pessoal, implicando um consumo em franco crescimento de recursos de processamento, armazenamento e transporte de dados (informação).

A informação é uma necessidade para ser acedida a qualquer hora e em qualquer lugar. As pessoas e as empresas investem em equipamentos e serviços de tecnologias da informação e comunicações (TIC) para serem utilizados nas suas atividades pessoais e profissionais, desde um simples armazenamento das fotos de viagem ao controlo financeiro de uma organização.

Manter uma infraestrutura de TIC não é tarefa simples e, muitas vezes, tem custos relativamente elevados. Este tipo de Infraestruturas requer investimentos em equipamentos de comunicação, armazenamento e outros sistemas que, além do custo inicial da sua aquisição, implicam complexidade na sua implementação, gestão e manutenção, exigindo profissionais qualificados e, consequentemente, também custos de exploração.

Algumas empresas sobressaem no cenário de desenvolvimento de produtos e sistemas de suporte à atividade pessoal e profissional, e/ou da sua implementação e manutenção como, e.g., sistemas operativos, editores de texto, aplicações, sistemas de comunicação escrita (falada e televisiva), plataformas específicas (para nichos de mercado) etc., favorecendo a atuação das empresas em novos tipos de negócio.

Por outro lado, existem ferramentas e plataformas completas distribuídas em código aberto, de livre utilização, com modelos e arquiteturas na nuvem e que podem, perfeitamente, cumprir as funções projetadas com elevado grau de qualidade e um custo relativamente reduzido.

No contexto digital, a segurança informática é um tema em constante desenvolvimento. As ameaças são cada vez mais sofisticadas e exigem das organizações um investimento constante e dispendioso para proteger os dados e as informações. O aparecimento de um sistema de regulamentação tem impacto na gestão das tecnologias, exigindo a adaptação das empresas a processos complexos com adoção de tecnologias (tipicamente) de elevado custo.

Os investimentos na proteção de dados são frequentemente alavancados, seja pela crescente preocupação com as ameaças no universo digital, como exposto no 'Relatório – Cibersegurança em Portugal – Sociedade 2020' (*CNCS - Relatório Sociedade 2020*, [s.d.]), ou pelas obrigações no cumprimento de normas, leis e regulações. Independentemente das razões, o facto é que os negócios familiares, as pequenas empresas e, num cenário muito especial, as *Startups*, têm que se adaptar para oferecerem a segurança necessária aos seus clientes e ao seu negócio.

Neste e-book, será abordada a Segurança Digital (SD) como um conjunto de medidas necessárias para a garantia da integridade das informações, cuja temática pode interessar aos mais diversos perfis profissionais (promotores, gestores e colaboradores) e empresariais, incluindo 'pequenas empresas', 'empresas familiares' e '*Startups*'.

É importante salientar que, qualquer trabalho de Segurança da Informação, deve ser conduzido através de uma análise criteriosa a ser desenvolvida especificamente para o ambiente alvo. As dicas, exemplos e recomendações presentes neste e-book têm o objetivo de proporcionar conhecimento para realizar análises críticas em cada ambiente e identificar potenciais fragilidades, assim como para ajudar a encontrar soluções eficazes de proteção para os seus dados e dos seus clientes.

Palavras-chave: Informação, dados, segurança digital, startups, organizações.

1. A INTERNET E OS NOVOS NEGÓCIOS

A presença na Internet é um fator diferenciador para qualquer negócio, uma vez que proporciona um meio de comunicação ágil e sem fronteiras. As pequenas empresas devem ser estimuladas a assegurar a sua presença na Internet desde o início.

Fotografia de Pickawood disponível em Unsplash

Notícias, marketing digital, comunicações pessoais e comerciais são uma constante com informação que é veiculada por todo o mundo. Atualmente, a informação flui com elevadas velocidades devido a toda a infraestrutura de comunicação existente (desde sistemas fixos a móveis terrestres e via-satélite). Os produtos e serviços online geram, diariamente, uma verdadeira avalanche de informações.

A sociedade tem alterado comportamentos em resultado da democratização das tecnologias móveis e da internet e está, por isso e cada vez, mais interligada. A figura 1.1 ilustra, a título de exemplo, esta evolução ao revelar imagens recolhidas com apenas oito anos de intervalo. Em 2005, a Igreja Católica Apostólica Romana perdeu o seu pontífice Papa João Paulo II e os fiéis aglomeraram-se na Praça de São Pedro, no Vaticano, à espera que fosse escolhido o novo líder da igreja. Alguns anos se passaram e o Papa Bento XVI renunciou ao pontificado em 2013, dando início novamente ao processo de escolha do novo líder, os fiéis concentraram-se mais uma vez na Praça de São Pedro, mas contribuíram significativamente mais para registar e disseminar a informação sobre o evento.

Fotografia de Camilo Jimenez disponível em Unsplash

Figura 1. Acesso digital entre os anos de 2005 e 2013

É notável a perceção da conectividade presente no evento no ano de 2013. A era digital consolida-se neste período. Há pessoas que estão a navegar na "rede" e com acesso a uma enorme quantidade de informação em tempo próximo do real, abrindo um universo de oportunidades e, por outro lado, devido ao volume e valor da informação, também surgem ameaças digitais mais complexas e robustas.

A presença na Internet é um enorme valor para qualquer negócio e o comércio eletrónico tem crescido num ritmo acelerado, conforme mostram as estatísticas publicadas pelo INE.

Em 2020, 61,5% das empresas com 10 ou mais pessoas têm website.

Fonte: Instituto Nacional de Estatística

A presença na Internet é um fator diferenciador para qualquer negócio, uma vez que proporciona um meio de comunicação ágil e sem fronteiras. As pequenas empresas devem ser estimuladas a assegurar a sua presença na Internet desde o início.

Entretanto, os pequenos negócios nem sempre têm a capacidade de realizar o investimento necessário para ter a sua própria infraestrutura ou plataforma de presença digital. Como solução para este cenário, surgem as ferramentas de comércio eletrónico baseadas na nuvem, comummente referida em inglês como cloud, que partilham recursos entre vários clientes, oferecendo produtos e serviços a preços mais acessíveis.
Portugal tem acelerado o crescimento do comércio eletrónico e já ultrapassou a média de crescimento da União Europeia (Figura 1.2).

COMÉRCIO ELETRÓNICO
% DO TOTAL DO VOLUME DE NEGÓCIOS

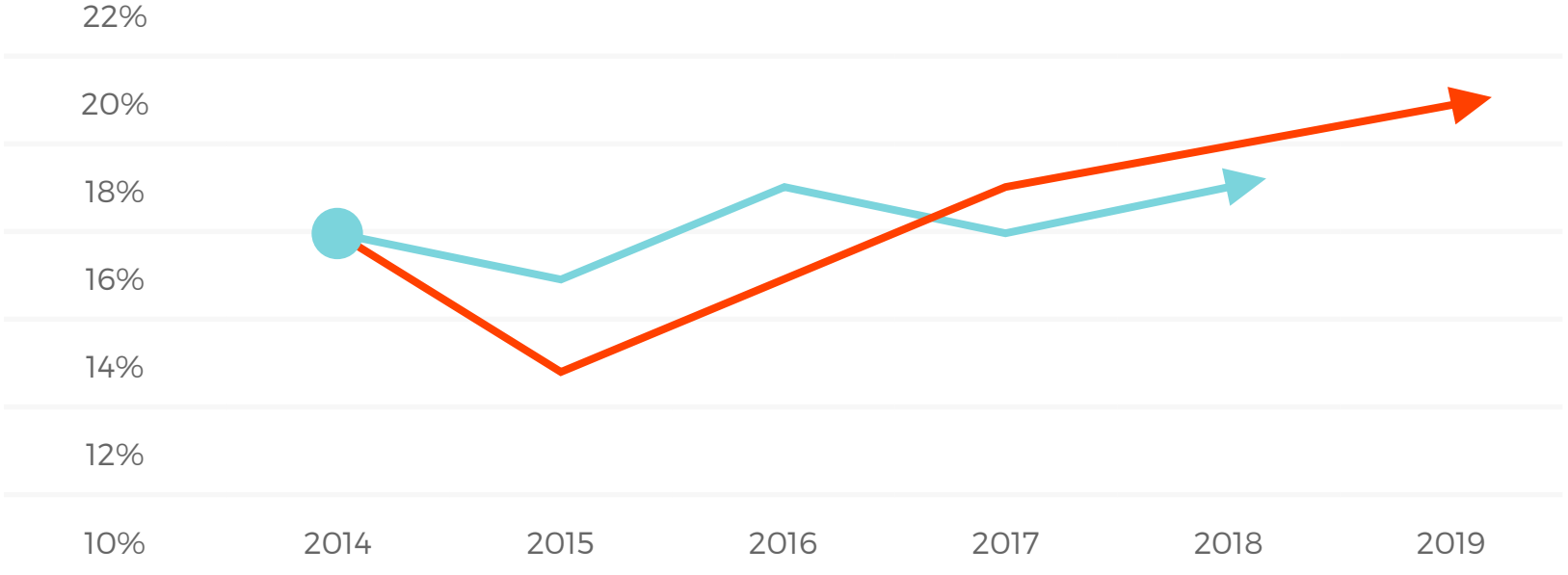


Figura 2. Inquérito à Utilização de Tecnologias da Informação e da Comunicação nas Empresas.
Fonte: Instituto Nacional de Estatística

A descrição dos produtos ou serviços e listas de preços foi a funcionalidade mais disponibilizada no website.

Fonte: Instituto Nacional de Estatística

De um modo geral, o termo informação liga-se intimamente ao conhecimento. Dir-se-á que, quem acede a uma maior quantidade de informação detém maior conhecimento. No plano dos negócios e das relações entre organizações, isso traduz-se na obtenção de vantagens relativamente a outras organizações, que podem ser de natureza política, financeira, económica ou tecnológica.

A prevenção de ameaças contribui decisivamente para a segurança de uma organização e por isso assume (nesse âmbito) um papel central; uma prevenção eficaz permite encetar todas as ações necessárias para impedir ou combater qualquer ameaça, e tal só é possível através de um serviço de informações bem estruturado.

Para além dos fatores financeiros, a insegurança digital, derivada de eventos amplamente divulgados, e.g., acerca da recolha não autorizada de dados pessoais, movimentos *hackers* e ameaças como vírus, despoleta nos clientes a necessidade de procura de empresas com competências especializadas em segurança da informação reconhecidas, através de selos de certificação e divulgadas em boletins públicos, que ofereçam confiança e garantia nos serviços e sigilo no tratamento de dados.

Fotografia de Stephen Dawson disponível em Unsplash

2. DADOS E INFORMAÇÃO

'Dado' é um elemento bruto que sem a correta interpretação não expressa qualquer significado. A informação pode ser entendida como dados dentro de um contexto que permite atribuir um significado, abstraindo o simples símbolo matemático e elevando-o a um entendimento no nível de raciocínio lógico e humano.

Para contextualizar o cenário da segurança, é necessário compreender o que são os dados e a informação. No artigo de SETZER, com o título "Dado, Informação, Conhecimento e Competência", dado é definido como:

> *«... uma sequência de símbolos quantificados ou quantificáveis. Portanto, um texto é um dado. De facto, as letras são símbolos quantificados ... um dado é necessariamente uma entidade matemática e, desta forma, é puramente sintático. Isto significa que os dados podem ser totalmente descritos através de representações formais, estruturais. Sendo ainda quantificados ou quantificáveis, eles podem obviamente ser armazenados num computador e processados por ele.»*
>
> Stzer, 2021

Desta abordagem, entende-se que dado é um elemento bruto, representado matematicamente e que, sem a correta interpretação, não expressa qualquer significado, sendo o dado capaz de conter informação.

O conceito de informação encontra várias definições na literatura académica, mas é consensual assumir que, dentro das empresas, pode ser entendido como um conjunto de dados integrados num contexto, que permite atribuir um significado, abstraindo-se do simples símbolo matemático, o que o eleva a um entendimento ao nível do raciocínio lógico e humano.

2.1. Dados pessoais

Os dados pessoais devemser especialmente observados e protegidos. Segundo a Comissão Europeia (*O que são dados pessoais?*, [s.d.]), os dados pessoais contêm "informação relativa a uma pessoa viva, identificada ou identificável. Também constituem dados pessoais o conjunto de informações distintas que podem levar à identificação de uma determinada pessoa."

DADOS PESSOAIS

O que são dados pessoais, dados sensíveis e dados comuns

DADOS PESSOAIS	DADOS SENSÍVEIS*	DADOS COMUNS
• Nome • E-mail (jose.silva@empresa.pt) • Número de telefone • Morada residencial • Endereços IP • Cookies	• Registo criminal • Registo médico • Raça ou etnia • Orientação sexual • Religião ou crenças • Filiação sindical	• Telefone da empresa • E-mail (info@empresa.pt) • NIF da empresa • Dados anonimizados • Informações de pessoas coletivas • Dados de uma pessoa morta

Figura 3. Dados Pessoais e Dados Comuns.

* Dados sensíveis são dados pessoais que têm a exigência de um tratamento especial.

2.2. Classificação dos dados

A informação pode ser classificada com base no seu domínio, ou seja, agrupada conforme o público a quem se destina, a relevância do seu conteúdo e as restrições aplicadas, encontrando-se na literaturadiversos modelos e segmentações da informação.

A informação é todo o conhecimento que possa ser comunicado e ao qual tenha sido atribuído um grau de classificação de segurança para proteção contra divulgação não autorizada.

A divulgação de informação classificada, independentemente do seu formato material ou modo de transmissão, poderá originar consequências geralmente adversas para o interesse da organização.

A classificação da informação (*Data Classification, 2016*) consiste na identificação do tipo de dado e na definição de níveis de proteção que cada dado deve receber, e.g., dados abertos, dados internos, dados do setor, dados confidenciais.

Diversos modelos foram criados para estabelecer uma classificação de dados que permita tratar as informações e aplicar o controlo adequado. Um exemplo de classificação pode conter os seguintes níveis de informação:

PÚBLICA	Informação que pode vir a público, sem consequências danosas significativas para o funcionamento normal da empresa, pelo que a sua integridade não é vital.
INTERNA	O acesso livre a este tipo de informação deve ser evitado, embora as consequências do uso não autorizado não sejam sérias. A integridade é importante, mesmo que não seja vital.
CONFIDENCIAL	Informação restrita aos limites da empresa, cuja divulgação ou perda pode levar a desequilíbrio operacional e, eventualmente, a perdas financeiras ou de confiabilidade perante o cliente externo.
SECRETA	Informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo, devendo o seu acesso ser restrito a um número reduzido de pessoas. A segurança desse tipo de informação é vital para a companhia.

Uma política base para um modelo de classificação de dados deve seguir minimamente os seguintes critérios:

- Ser direta e evitar ambiguidade. Porém, a política utilizada deve ser genérica o suficiente para aplicação a diferentes ativos em vários contextos;
- Ser clara e escrita de forma simples;
- Estar alinhada com o negócio da organização;
- Conter poucas páginas e não ter mais do que três ou quatro níveis de classificação;
- Conter o ponto de contacto para os mais diversos casos e situações que os funcionários podem enfrentar;
- Conter uma agenda de revisão.

2.3. Proteção dos dados

A proteção dos dados consiste na criação de controlo de segurança para dados classificados de natureza pessoal, ou qualquer outro dado sensível para o negócio. Por exemplo, os relatórios financeiros da empresa devem ter controlo de acesso e serem mantidos na guarda das tecnologias de proteção.

Especialmente depois da aprovação da Lei Geral de Proteção de Dados (LGPD) e entrada em vigor do Regulamento Geral de Proteção de Dados (RGPD) na Europa, alguns países exigem medidas extraordinárias de proteção de dados, por parte de parceiros e investidores que recolham informações dos seus cidadãos.

Para minimizar os riscos, devem ser recolhidos os dados estritamente necessários para o negócio, mantidos em segurança, com registado dos acessos e transmitidos apenas por meios seguros. Em casos de desastre, a recuperação de dados deve ser realizada de forma a ter toda a informação reposta em tempo de forma a minimizar o impacto para o negócio.

2.4. Continuidade do negócio e recuperação de desastres

As organizações que possuem um plano de continuidade de negócio (bem pensado e estruturado), garantem a sua capacidade de resposta em caso de eventos inesperados e, consequentemente, a sustentabilidade do seu negócio.
Não existem fórmulas fechadas que garantam um "antídoto eficaz" no caso de uma organização ser afetada por um ciber ataque, uma catástrofe natural ou um ataque terrorista. Mas há decisões de investimento que só podem ser tomadas se existir conhecimento dos recursos que disponíveis para que um gestor possa, de forma consciente, preparar melhor a sua empresa para as eventualidades do futuro.

2.5. Arquitetura de TI

O alinhamento das necessidades do negócio com as tecnologias depende da estrutura da Arquitetura de TI como uma competência da tecnologia da informação que garante que os processos e as soluções tecnológicas são adequados às necessidades das organizações, gerando conformidade e alinhamento com os objetivos estratégicos e, por outro lado, assegurando que a área de TI está a contribuir para beneficiar agilmente o desenho do modelo de negócios, dos processos e de tecnologias, nomeadamente para:

- Planear arquiteturas de infraestrutura adequadas para o negócio;
- Lidar com sistemas já implementados e integrá-los nas novas tecnologias;
- Implementar um novo sistema de armazenamento com classificação dos dados;
- Garantir um manuseamento responsável dos dados na organização;
- Implementar e gerir soluções eficientes e inovadoras;
- Implementar redes, routers, firewalls e servidores físicos e virtuais.

3. REGULAMENTO GERAL SOBRE A PROTEÇÃO DOS DADOS

O Regulamento Geral sobre a Proteção de Dados (RGPD) apresenta um conjunto único de regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação dos mesmos. Estão sujeitas à sua aplicação as empresas estabelecidas na UE, independentemente da sua localização

Fotografia de Taylor Vick disponível em Unsplash

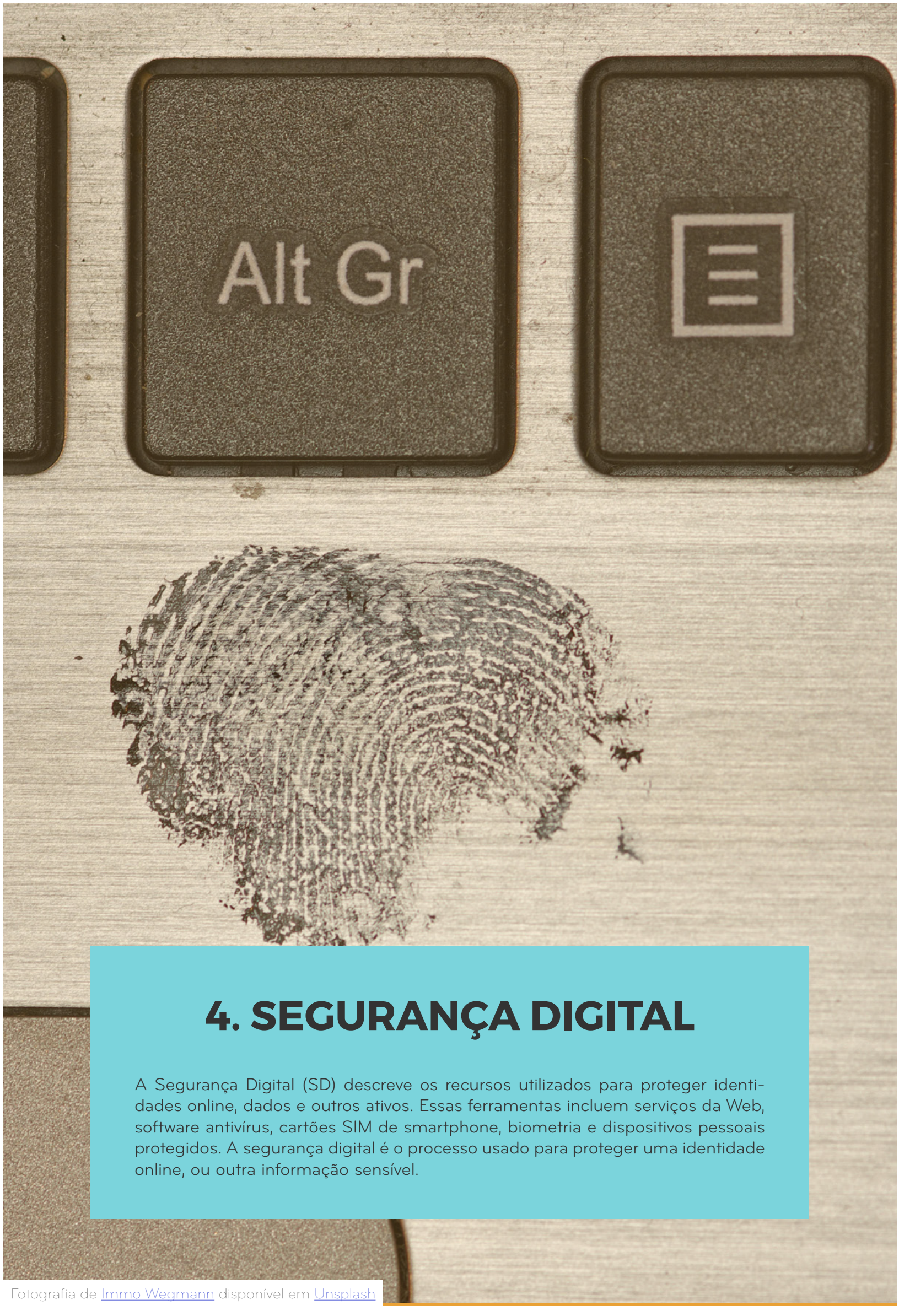
Fotografia de ricochet64. Créditos: Getty Images/iStockphoto.

- O Regulamento Geral sobre a Proteção de Dados (RGPD) apresenta um conjunto único de regras relativas à proteção das pessoas singulares, relativamente ao tratamento de dados pessoais e à livre circulação desses dados. Estão sujeitas à sua aplicação as empresas estabelecidas na UE, independentemente da sua localização geográfica (*IAPMEI - Regulamento Geral de Proteção de Dados*, [s.d.]).

- No artigo 30º, o RGPD define a obrigatoriedade em registar as atividades de tratamento de dados pessoais. Isto significa que, sempre que estabelecida uma relação comercial, e uma entidade solicitar dados pessoais de utentes/clientes, deve-se lançar um processo de registo dos dados recolhidos e indicar a finalidade para a qual estes dados serão utilizados, com o respetivo registo do consentimento do titular dos dados.

- Em Portugal, a Comissão Nacional de Proteção de Dados (CNPD) é o organismo que tem por atribuição controlar e fiscalizar o cumprimento do RGPD e da lei que o executa na ordem jurídica portuguesa, 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 de dados pessoais.

As normas e legislações específicas como o RGPD trazem variáveis complexas para a inserção das empresas no mercado, sobretudo quando estas estão no ambiente digital.



4. SEGURANÇA DIGITAL

A Segurança Digital (SD) descreve os recursos utilizados para proteger identidades online, dados e outros ativos. Essas ferramentas incluem serviços da Web, software antivírus, cartões SIM de smartphone, biometria e dispositivos pessoais protegidos. A segurança digital é o processo usado para proteger uma identidade online, ou outra informação sensível.

Fotografia de Immo Wegmann disponível em Unsplash

A Segurança Digital (SD) descreve os recursos utilizados para proteger identidades online, dados e outros ativos. Essas ferramentas incluem serviços da Web, software antivírus, cartões SIM de smartphone, biometria e dispositivos pessoais protegidos. A segurança digital é o processo utilizado para proteger uma identidade online. A SD é aplicada como uma componente da Segurança da Informação.

A Segurança da Informação é um conjunto de áreas que se refere à proteção de informações de uma empresa ou pessoa. Entende-se por informação, qualquer dado que devidamente interpretado, transporte consigo algum conhecimento, sendo importante conhecer os seus modelos de dados, as informações que estão codificadas nestes modelos e classificá-los devidamente para aplicar o tratamento mais adequado.

A segurança é baseada em três pilares tradicionais:

A Confidencialidade
É uma propriedade que visa garantir que o acess
quem tem o direito ao mesmo.

A Disponibilidade
É uma propriedade que tem por objetivo, garan
requisitados (apenas para os utilizadores devidam

A Integridade
É uma propriedade definida para garantir que a info
desde a sua geração até o fim do seu ciclo de vi

Após a identificação e mapeamento de todos o
segurança e selecionar os meios onde serão mar

A Política de Segurança deve conter pelo menos

Fotografia de Luther.M.E. Bottrill disponível em Unsplash

- Análise do ambiente interno;
- Matriz de responsabilidades;
- Análise SWOT;
- Análise de impacto do negócio;
- Plano de formação e consciencialização;
- Indicadores-chave de desempenho.

Para cada controlo de segurança aplicado, é importante identificar e mapear o impacto daquela componente no negócio.

5. AMEAÇAS E RISCOS

Quanto mais a empresa depender das Tecnologias da Informação, mais importante será identificar e controlar os riscos relacionados com os seus ativos informáticos para evitar potenciais prejuízos para os seus negócios.

Fotografia de Setyaki Irham disponível em Unsplash

Em muitos países, as *Startups* agregam uma parte considerável do capital intelectual e têm um papel relevante para o crescimento e resiliência da economia. Não é raro que essas empresas enfrentem restrições financeiras e de pessoal e, como consequência, colocam a cibersegurança (Cibersegurança, 2020) como uma baixa prioridade nos produtos ou serviços. Infelizmente, basta um ataque ou violação de segurança bem-sucedidos para destruir a reputação da *startup*, mesmo antes desta estar implantada no mercado.

Assim como ocorre com as pequenas empresas, as *Startups* enfrentam desafios únicos e a cibersegurança não é uma exceção. Desde a compreensão da sua exposição ao risco, até a localização e mobilização de recursos apropriados para mitigá-lo, muitos empresários lutam para manter sua empresa segura com um orçamento limitado e para construir a confiança do cliente enquanto constroem seus negócios.

Estas empresas são vistas como "presas fáceis" e interessantes pelos cibercriminosos porque, além de possuírem informações que estes podem utilizar, muitas vezes não têm uma infraestrutura de segurança que as empresas de maior dimensão dispõem. Por outro lado, uma pequena empresa é vista como um possível veículo de ataque a uma empresa de maior dimensão, com a qual se relacione.

A cibersegurança deveria estar no topo das preocupações para a maioria dos proprietários de *Startups*, principalmente em tempos em que crimes cibernéticos e ataques à privacidade de dados tornaram-se rotina. O estabelecimento e manutenção de uma relação de confiança com os clientes é um desafio contínuo e construída negócio a negócio, transação a transação, mas esta pode ser comprometida em caso de ocorrência de um incidente de segurança.

Ao priorizar a cibersegurança, o empreendedor terá a oportunidade de ver a sua empresa crescer robusta e capaz de suportar ameaças e ataques cibernéticos cada vez mais sofisticados e frequentes.

Quanto mais um negócio depender das Tecnologias da Informação e Comunicação (TIC), mais importante será identificar e controlar os riscos relacionados aos seus ativos de tecnologia. Os riscos associados às TIC referem-se à probabilidade da ocorrência de eventos ou incidentes (falhas de equipamentos, falta de energia elétrica ou ataques maliciosos de hackers, entre outros) que têm o potencial de interromper sistemas críticos de apoio aos processos de negócios ou permitir acesso não autorizado aos ativos de informação da sua organização, dos seus fornecedores ou clientes.

No âmbito da cibersegurança existem cinco recomendações importantes para proteção e ataques conforme visto na Figura 4.

DICAS PARA PROTEÇÃO CONTRA AMEAÇAS CIBERNÉTICAS

REVISÃO	SOFTWARE	SENHAS	NÃO RESPONDA	NÃO ABRA
Reveja as suas contas online e configure alertas para acessos incomuns	Instale software antivírus e mantenha o sistema atualizado	Crie senhas complexas com letras, números e caracteres especiais	A e-mails, SMS e telefonemas de origem não conhecida	Anexos ou links enviados por e-mails desconhecidos

Figura 4. Recomendações para proteção no âmbito da cibersegurança

As violações de segurança podem devastar até mesmo as empresas mais resilientes. Os eventos desta natureza podem resultar em perdas financeiras decorrentes, entre outros fatores, de:

- Roubo de fundos e de informações estratégicas ou financeiras;
- Perdas de vendas pela interrupção dos processos de negócio;
- Danos à reputação da empresa: redução de vendas e lucros pela perda de confiança por parte de clientes, fornecedores ou parceiros de negócios;
- Multas e sanções regulatórias resultantes do não cumprimento dos requisitos legais aplicáveis ao seu segmento de negócios ou às leis de proteção de dados e privacidade;
- Ações legais individuais ou coletivas por falhas na proteção da informação de clientes ou parceiros;
- Custos associados à reparação de sistemas, redes e dispositivos afetados, ou outras atividades ou serviços necessários para que os processos de negócio voltem ao seu estado operacional normal, que poderão incluir até o pagamento de resgate aos hackers (hackers, 2021).

A gestão de riscos cibernéticos é uma prioridade central nos negócios, para que a probabilidade de ocorrência de eventos negativos seja reduzida, as suas possíveis consequências sejam eliminadas ou controladas, e o retorno à operação normal aconteça no menor tempo possível. A seguir, apresentaremos as etapas básicas do processo de gestão de risco cibernético, as principais ameaças a que estão expostas as organizações e estratégias para eliminar ou mitigar as suas consequências.

5.1. Gestão de risco cibernético

Fotografia de Michael Geiger disponível em Unsplash

Atualmente, muitos dos serviços associados a tecnologias da informação podem ser contratados a entidades terceiras, inclusive os relacionados com cibersegurança. A aquisição de serviços de cibersegurança não significa transferir toda a responsabilidade pela segurança (ou pela sobrevivência da empresa) para o contratado. Neste sentido, é necessário um acordo do negócio e dos riscos subjacentes a este, de forma a conceber e validar um planeamento com as várias fases para a sua implementação, para que as organizações fiquem preparadas para o risco cibernético.

Como primeiro passo, as startups devem considerar abordagens estruturadas ao risco. O NIST Cybersecurity Framework, Figura 5, fornece uma linguagem comum para compreensão, gestão e expressão do risco cibernético. Em seguida, devem ser identificados e rastreados os ativos de tecnologia (hardware, software) e de informação (dados dos clientes e fornecedores; propriedade intelectual, dados financeiros, estratégia da empresa) e entender o valor destes ativos para o seu negócio. Sem esse rastreamento de ativos, o controlo de acesso e configuração e as políticas de gestão de segurança perderão eficácia. A questão seguinte a ser respondida é se os ativos de tecnologia e informação (anteriormente identificados) estão devidamente protegidos. Se a empresa utiliza serviços baseados na nuvem, é importante assegurar que o seu contrato com o fornecedor destes serviços tenha os âmbitos e responsabilidades, relativos à cibersegurança, claramente definidos e que estejam de acordo com os requisitos do negócio.

Figura 5. Framework do NIST

A partir deste ponto, ações deverão ser executadas para resolver os desvios identificados, sempre na perspetiva das necessidades de negócios e da sua capacidade de investimento. A seguir, apresentam-se as etapas gerais de um processo de gestão de risco cibernético, a partir da definição geral de risco e da necessidade de controlo e atualização permanentes.

Na norma ISO 31000:2018, risco é definido como "o efeito da incerteza nos objetivos". O risco pode ser caracterizado de acordo com a sua origem (fonte), eventos potenciais, as suas consequências e possibilidade de ocorrência. O seu efeito nos objetivos pode ser positivo, negativo ou ambos, e abordar ou criar ameaças ou oportunidades para uma organização ou processo de negócio.

A gestão de risco, de forma geral, é o processo que identifica, avalia e controla ameaças aos recursos, capital e ganhos de uma organização. Na gestão de riscos cibernéticos, os princípios gerais da gestão de risco são aplicados à organização de TI, através de políticas, procedimentos e tecnologias para reduzir ameaças, vulnerabilidades de ativos tecnológicos e dados desprotegidos e as suas respetivas consequências.

A gestão de risco consiste em vários processos para criar resiliência e desenvolver na empresa a capacidade de prevenir, detetar e responder aos eventos relacionados com os ativos e dados, de forma a minimizar a interrupção dos negócios e a consequente perda financeira. Estes processos incluem as seguintes etapas:

- Identificar os ativos tecnológicos e de dados que podem tornar-se alvos de criminosos cibernéticos ou ser impactados por eventos naturais, devido às vulnerabilidades que apresentam;

- Identificar o maior número possível de riscos a que o negócio está exposto no seu ambiente operacional. Os riscos cibernéticos ou de TI incluem falhas de software e hardware, ataques maliciosos (vírus, spam, entre outros), erro humano e desastres naturais (e.g., inundações, incêndios, tempestades);

- Analisar cada fator de risco identificado para determinar o seu âmbito e a sua relação com os diferentes fatores dentro da organização e mapear quais os processos de negócio afetados por um determinado risco e qual é a amplitude do impacto causado. Fatores que impactam o risco cibernético de uma organização incluem, entre outros, as regulamentações e outros requisitos legais afetos ao segmento de indústria e local em que opera, o seu modelo de negócio, produtos ou serviços oferecidos, plataforma tecnológica adotada e localização dos clientes e fornecedores;

- Classificar e priorizar o risco. Existem riscos que, se concretizados, podem paralisar todo o negócio, enquanto existem riscos que serão apenas pequenos inconvenientes e, portanto, aceitáveis. A classificação dos riscos permite que a organização obtenha uma visão holística da exposição ao risco a ser usada na priorização das ações e investimentos a serem feitos para tratá-los;

- Tratar os riscos com medidas que possam ser eliminados ou contidos, na medida do possível. No caso dos riscos cibernéticos, deverão ser implantadas as medidas de cibersegurança necessárias, sejam elas de natureza técnica (aquisição de tecnologia), processual ou para as pessoas da organização (formação técnica, campanhas de consciencialização sobre cibersegurança);

- Monitorizar e analisar o risco, uma vez que os riscos não são estáticos e a eficácia das medidas de tratamento pode ser negativamente impactada por mudanças no ambiente interno ou externo da organização. Os processos e indicadores associados ao tratamento dos riscos devem ser definidos e monitorizados, e os eventuais desvios identificados ser usados para ajustes e/ou criação de medidas preventivas ou corretivas de tratamento de riscos;

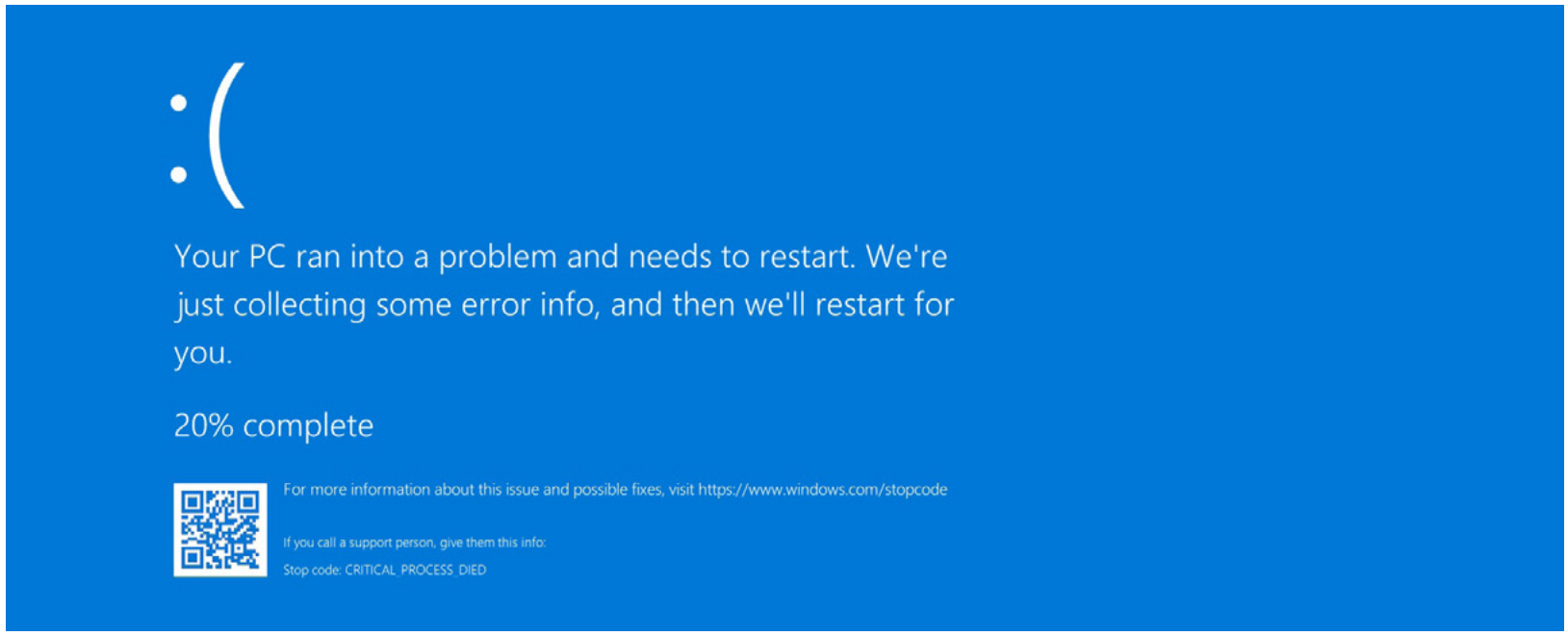
Atualmente, uma empresa tem a oportunidade de optar por implementar um sistema de gestão de riscos cibernéticos para implementar boas práticas na prevenção de ataques cibernéticos e obter uma certificação, para garantir aos clientes que são adotadas medidas, ou melhores práticas para sistemas de gestão de cibersegurança.

A norma ISO 27001 (ISO 270001, 2013) é uma norma internacional que descreve as melhores práticas para sistemas de gestão de segurança da informação. Esta norma é parte da família de ISO 27000, cujo objetivo é ajudar a manter protegidos os ativos de informação de uma empresa. A norma ISO 27001 especifica o controlo essencial para manter a segurança, nomeadamente: política de segurança, classificação e controlo de ativos, segurança física e ambiental - controlo físico de acesso a informações e equipamentos, segurança do ambiente de trabalho, controlo de identidade e acesso, desenvolvimento e manutenção do sistema, gestão de continuidade de negócios e conformidade com as leis nacionais e internacionais relevantes.

5.2. Ameaças cibernéticas mais comuns para pequenas empresas

Os dois tipos mais comuns de ameaças para pequenas empresas são engenharia social e *malware* (malware, 2021). Engenharia social é a manipulação dos indivíduos, geralmente através de e-mail, telefone ou mensagem de texto (SMS), para obter informações confidenciais (e.g., como credencias de login) ou induzir uma ação como, e.g., clicar num link e fazer o download de um ficheiro ou visitar uma página web maliciosa onde o hacker pode implantar *ransomware* (ransomware, 2021) ou outro malware.

5.2.1. Malware



Malware (*software* malicioso) é um termo abrangente que se refere a software projetado para causar danos num computador, servidor, cliente ou rede de computadores, para dar aos cibercriminosos acesso ao sistema da vítima. O *malware* pode incluir vírus e *ransomware*.

Os vírus são programas maliciosos que se espalham de computador para computador (e outros dispositivos interligados). Os vírus são projetados para dar aos cibercriminosos acesso ao sistema da vítima.

Ransomware é um tipo específico de *malware* que bloqueia o computador da vítima ou cifra todos os seus dados até que o resgate seja pago. O *ransomware*, geralmente é entregue por meio de um link malicioso pela via de um e-mail e explora vulnerabilidades não corrigidas no *software*. Frequentemente, os dados ou sistema não são restaurados, mesmo após o resgate ser pago.

5.2.2. Ameaças por email

Phishing é um tipo de ataque de engenharia social que utiliza o e-mail, ou um site malicioso, para infetar uma máquina com um *malware* ou recolher informações confidenciais. Os emails de *phishing* aparecem como se tivessem sido enviados por uma pessoa conhecida ou de uma organização legítima, induzindo os utilizadores a clicar num link ou abrir um ficheiro que contém código malicioso.

5.2.3. Ameaças em ambientes de videoconferência

Historicamente, as pequenas empresas contam com ferramentas para dar suporte a escritórios virtuais e funcionários remotos. Com a crise do COVID-19, um elevado número de pessoas recorreu às plataformas de videoconferência (VTC) para interagir com outras pessoas em âmbito pessoal ou profissional. Alguns relatos de conferências interrompidas por imagens pornográficas e/ou de ódio e linguagem ameaçadora tornaram-se mais frequentes nos últimos meses.

Os eventos virtuais são um ambiente no qual as técnicas de engenharia social podem ser aplicadas para informações que poderão facilitar um futuro ataque cibernético.

5.3. Vulnerabilidades cibernéticas

Uma vulnerabilidade é uma fraqueza que pode ser explorada por um agente malicioso com o objetivo de obter acesso ou executar ações não autorizadas num sistema ou dispositivo. As vulnerabilidades podem permitir que os *hackers* executem programas, instalem *malware* e copiem, modifiquem, cifrem ou destruam dados. As vulnerabilidades mais comuns (para pequenas empresas) incluem as comportamentais, injeção de código, exposição de dados confidenciais, proteção de *endpoint* e a gestão de identidades.

As vulnerabilidades aumentam a superfície de ataque de uma organização, ou seja, os pontos com potencial de exploração por agentes mal-intencionados. Os sites públicos, dispositivos pessoais e pessoas são elementos principais de uma superfície de ataque. Para a reduzir, as organizações devem avaliar regularmente as suas vulnerabilidades e identificar os pontos fracos de segurança, além de monitorizar anomalias na rede e em servidores.

A análise das vulnerabilidades, das fraquezas e dos procedimentos de mitigação deve ser uma rotina constante, cíclica e perene no ambiente informático das empresas.

5.3.1. Vulnerabilidades comportamentais

A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de utilização de quem a acede, pelo ambiente ou infraestrutura, que a cerca ou por pessoas mal-intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

O erro do utilizador final é a principal ação de ameaça à segurança e trata-se de uma questão significativa para as organizações de qualquer dimensão. As vulnerabilidades (pontos fracos) comportamentais incluem:

- Utilização de senhas "fracas";
- Clicar em links maliciosos recebidos por email;
- Navegar em sites não seguros;
- Fazer o download de ficheiros maliciosos;
- Falhar em cumprir as medidas prescritas para proteger informações confidenciais;
- Falhar na atualização dos softwares dos sistemas.

A melhor forma de mitigar vulnerabilidades comportamentais é através do treino e da consciencialização sobre segurança para o utilizador final. A consciencialização em segurança da informação é um dos tópicos mais destacados dos últimos anos, especialmente devido à crescente de dispositivos *Internet of Things (IoT)* e do trabalho remoto.

A ação de consciencializar a comunidade organizacional sobre a natureza do negócio da empresa, especificamente sobre as potenciais ameaças, riscos e comportamentos que promovem um ambiente mais seguro é fomentar a segurança da informação.

Sem recursos suficientes para investir em ferramentas e sistemas sofisticados de cibersegurança, as formações em segurança fornecerão os melhores resultados para pequenas empresas. Muitos programas de formação estão disponíveis para ajudar a reforçar os conceitos de segurança. É essencial rastrear as taxas de sucesso, ou falha, de um utilizador nos testes, bem como nos testes de "fogo real" com e-mails de *phishing* e outras táticas.

A Segurança é um dever de todos os colaboradores para com a organização e os seus ativos de informação. Cada indivíduo deve observar regras e condutas de segurança ao tratar os dados da organização. Por este motivo, é importante manter a comunidade organizacional sempre ciente das ameaças, formas de identificar e com um canal direto de comunicação com a gestão das tecnologias da informação, para reportar qualquer indício de risco e potenciais ataques, antes de estes causarem maiores impactos no negócio.

5.3.2. Injeção de código

Os ataques de injeção de código estão entre os mais comuns. Existem vulnerabilidades que permitem aos cibercriminosos injetar código malicioso no sistema da vítima, explorando aplicações que permitem entradas do utilizador em bases de dados, comandos de *shell* ou sistema operacional.

A monitorização de padrões de comportamento anormal de dados de entrada, em sistemas de computação, é uma estratégia de mitigação eficaz para ataques de injeção de código. Existem antivírus (de última geração) que procuram ações não consistentes com os padrões da entrada de dados feita por humanos e também padrões de comportamento que são utilizados por agentes mal-intencionados. Este tipo de ferramentas fornece uma análise abrangente do comportamento malicioso, além de opções de prevenção e deteção mais flexíveis.

5.3.3. Proteção de dados confidenciais

A falha humana em tomar as precauções prescritas para proteger dados confidenciais também adiciona uma camada de vulnerabilidade. Os dados gravados nos dispositivos de armazenamento e também os dados em trânsito, devem ser protegidos. Os especialistas em segurança recomendam que os dados, confidenciais ou sensíveis, sejam armazenados em formato cifrado. Contudo, mesmo os dados cifrados são suscetíveis a um ataque de *ransomware*.

Cifrar dados não é um empreendimento dispendioso, e as pequenas empresas devem seguir as práticas recomendadas para a utilização de criptografia para proteger os dados. Usar uma VPN para criptografar dados (à medida que são transmitidos) é uma solução comum e eficaz, assim como manter os dados cifrados em repouso, mesmo quando o controlo de acesso, ao nível dos utilizadores e senhas, falham.

Adicionalmente, recomenda-se implementar criptografia em vários níveis, e.g., na base de dados e no dispositivo físico de armazenamento onde reside a base. As chaves de criptografia de dados devem ser atualizadas com regularidade e ser armazenadas separadamente dos dados.

Uma solução que muitas pequenas empresas consideram satisfatória, para proteger os dados em trânsito, é o uso de drives flash criptografados. Se os dados criptografados forem necessários num local remoto, mover fisicamente as informações numa unidade criptografada pode ser a solução certa em algumas circunstâncias.

Para proteger os dados contra *ransomware*, recomenda-se uma estratégia de *backup* e recuperação multifacetada, que inclua dados do sistema, *backups* de base de dados e dos dados do utilizador final.

5.3.4. Dispositivos endpoint

Os computadores portáteis e desktops, tablets e telefones móveis interligados na rede da organização são potenciais vetores para *malwares*. O nível de atualização do *software* instalado, as aplicações instaladas (em cada dispositivo *endpoint*) e a sua conformidade com as políticas de segurança irá definir o nível de exposição, inclusivamente em pequenas empresas.

Ao desenvolver e implementar políticas que obriguem a que todas as aplicações e sistemas operacionais de qualquer *endpoint* (ligado à rede de negócios) sejam atualizados e corrigidos é a medida de proteção de *endpoint* mais eficaz e menos dispendiosa.

Definir expectativas claras para a segurança do *endpoint* é vital para evitar mal-entendidos futuros e não conformidade com políticas em casos do uso pessoal e comercial de um mesmo dispositivo *endpoint*.

5.3.5. Gestão de credenciais

Uma das causas mais comuns de comprometimento do sistema é a falta de uma gestão robusta de credenciais. A utilização da mesma senha para várias contas, até mesmo reutilizando senhas de contas pessoais em sistemas comerciais, representa uma das vulnerabilidades mais exploradas pelos hackers que podem usar as credencias obtidas em violações anteriores para tentar logins numa vasta variedade de sites.

Para a maioria das organizações, resultados satisfatórios podem ser alcançados com a implementação de controlo rigoroso de senha, e.g., a utilização de senhas mais longas, mais complexas, forçando alterações de senha mais frequentes ou uma combinação desses princípios. Atualmente, a Autenticação Multi-factor (*Multi-Factor Authentication - MFA*) é utilizada em vários serviços, como um mecanismo adicional de autenticação de um utilizador. Em poucas palavras, a MFA é a utilização de dois ou mais fatores, ou métodos, para verificação quanto à autenticidade de algo ou de uma pessoa.

Redes sociais (com o Facebook) e os principais serviços de e-mail (Gmail do Google) e mesmo no mundo físico, como terminais ATM (em alguns países), já utilizam mais do que um meio para certificar-se que o utilizador que está a tentar aceder ao serviço está autorizado. Existem algumas alternativas que podem ser adotadas como um segundo, terceiro ou n-ésimo fator de autenticação:

- Ao nível da Biometria (leitura de impressões digitais, leitura de íris ou retina ou reconhecimento facial);
- Códigos de verificação enviados para uma conta de email ou SMS;
- *Tokens* gerados por *hardware* ou *software*;
- Certificados embutidos em *smart cards*.

A utilização de ferramentas de gestão de senhas ajuda e facilita a adoção de políticas de gestão de senhas. Estas ferramentas eliminam a necessidade de os utilizadores terem de se lembrar de um elevado número de senhas.

6. SOLUÇÕES E TENDÊNCIAS

Na era digital, a necessidade de segurança digital implica a procura de soluções de segurança eficazes (plataformas e pacotes de software atualizados) que garanta a confiança dos responsáveis das empresas relativamente aos seus negócios e aos seus dados. Um conjunto de soluções e tendências são referidos como investimento na área da segurança digital.

Fotografia de Diego PH disponível em Unsplash

Como descrito anteriormente, a limpeza de dados poderá implicar custos significativos, tanto financeiros como de reputação. A proteção dos dados da empresa e dos clientes é uma parte fundamental para o plano de negócios da Cibersegurança, não sendo necessário ser dispendiosa, mas exige esforço e diligência na execução.

Uma plataforma de segurança eficaz tem, na sua base, componentes de simples implementação e custos relativamente acessíveis. Neste sentido, indicam-se algumas sugestões de investimento:

Antivírus e antimalware confiável

Um dispositivo comprometido significa exposição a ataques. Cada ação, desde o login no e-mail até a verificação do saldo da conta bancária da sua empresa, são situações de potencial exposição. Instale um *software* antivírus e *antimalware* confiável em cada portátil, desktop ou telemóvel em utilização por cada colaborador.

Autenticação multi-factor (MFA)

Como abordado anteriormente, o MFA apresenta um ou mais requisitos adicionais de identificação para acesso a serviços, exigindo, e.g., uma senha e um código, que pode ser enviado como uma mensagem de texto para um número de telefone especificado pelo utilizador. Para todos os principais serviços na nuvem é importante a sua ativação. A Google, Amazon e Microsoft fornecem orientações (passo a passo) para configuração e utilização da MFA.

Criptografia para proteger dados sensíveis

Se uma empresa armazena qualquer tipo de dados de clientes, sejam informações regulamentadas (e.g. números de cartões de crédito, ou simplesmente dados pessoais, endereços de entrega), é conveniente cifrar a base de dados em todo o processo da entrada para a saída. É conveniente a utilização de criptografia forte nos sistemas de produção e logística.

Segurança como parte da cultura organizacional

Um dos elos mais fracos de qualquer sistema de segurança não é tecnológico, mas o humano. A maneira mais conveniente e frequente de atacar a segurança da maioria das organizações é através da equipa; 93% de todos os ataques começam com um e-mail utilizado para enviar *malware* para um dispositivo. A melhor abordagem, nestes casos, é consciencializar a equipa dos riscos e de que a liderança da empresa leva a segurança a sério, e do protocolo definido para tratamento de e-mails ou telefonemas suspeitos, e até mesmo de tentativas de entrar nas instalações físicas.

DICAS PARA PROTEÇÃO CONTRA AMEAÇAS CIBERNÉTICAS

ATENÇÃO	SITE SEGURO	ATENÇÃO	SENHA SEGURA
A websites falsos e links suspeitos	Verificar o site no navegador	Para e-mails de *phising*	Crie senhas fortes
REDES SOCIAIS	**ADWARE**	**BANCOS**	**SOFTWARE**
Valida os acessos às redes sociais	Previna-se contra adwares	Configure acessos seguros	Atualize os seus sistemas

Figura 6. As 8 dicas para uma navegação segura

Procure ajuda

É especialmente importante para as Startups ou para quem está a trabalhar com dados sensíveis, procurar ferramentas que automatizam a deteção de ameaças que possam reduzir o tempo e o esforço para identificar violações de segurança. É melhor, e quase sempre menor, o custo de prevenir a remediar, i.e., na prevenção e na reparação. A inclusão de plataformas específicas no arsenal de cibersegurança, pode ser uma mais-valia para a empresa. Contudo, a cibersegurança tende a tornar-se um tema complexo à medida que a empresa cresce e aumenta a probabilidade de sofrer ataques. Há uma série de empresas focadas em fornecer "inteligência contra ameaças" automatizada, ao lado de serviços e ferramentas mais tradicionais que lidam com a monitorização e gestão de segurança no modelo "*as a service*". O portefólio de serviços de segurança destas empresas pode incluir, e.g., a avaliação de risco; gestão de risco; treino e consciencialização; proteção de *endpoints*; segurança de e-mail; gestão de segurança em nuvem; gestão de acesso (físico e/ou digital); *firewall* e rede; criptografia de dados; monitorização, deteção e resposta de incidentes de segurança; teste de penetração (*pentests*); etc.

Seguro Cibernético

O seguro de cibersegurança, seguro de responsabilidade cibernética ou seguro cibernético, é uma modalidade de seguro que uma empresa pode adquirir para ajudar a reduzir os riscos financeiros associados à realização de negócios online, ao transferir (mediante o pagamento de um valor), parte do risco para a seguradora.

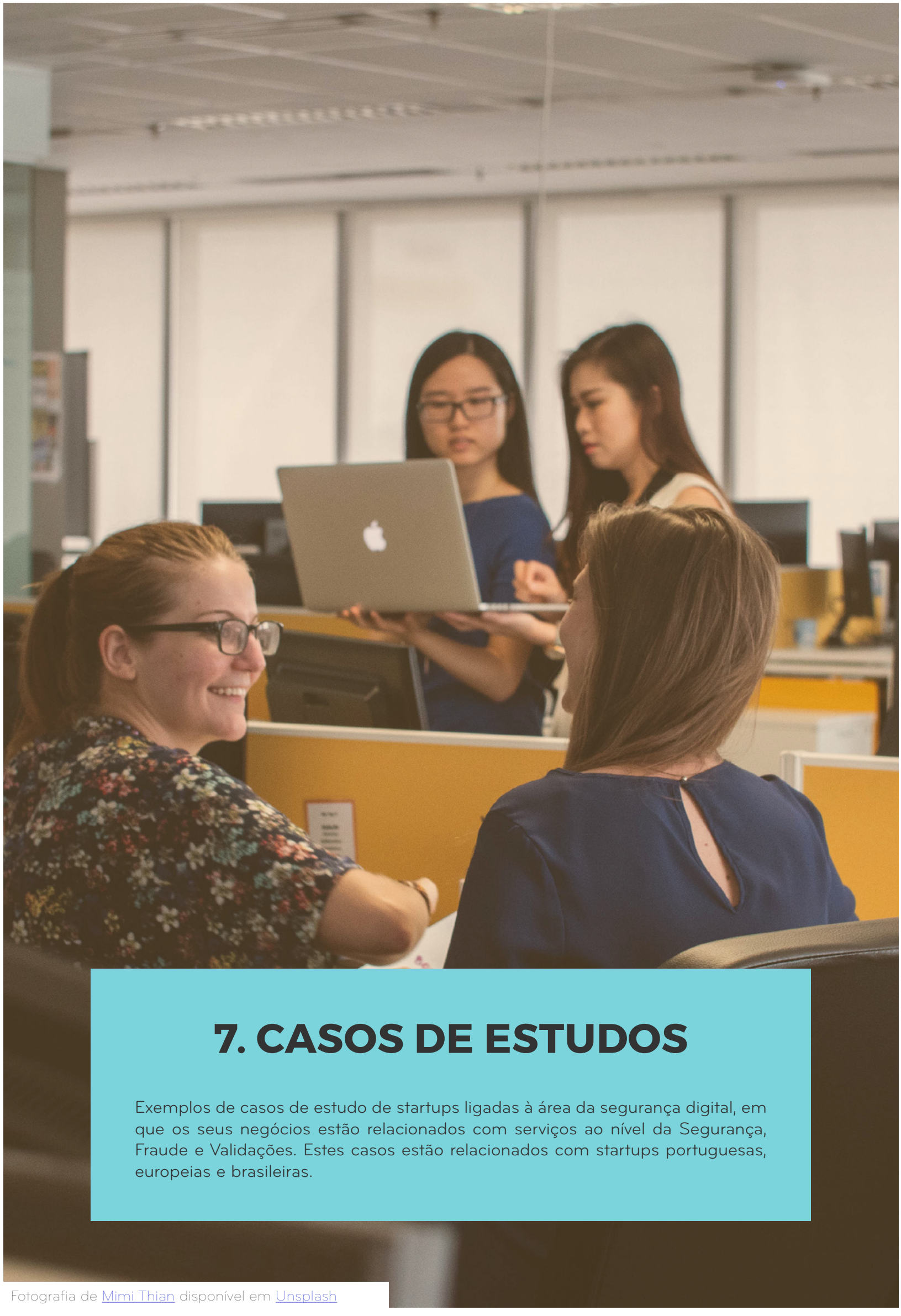
Em geral, as apólices incluem cobertura primária para as perdas que se aplicam diretamente a uma empresa, e cobertura de terceiros aplicável a perdas sofridas por terceiros em evento ou incidente cibernético, com base no relacionamento comercial existente, com a empresa que adquiriu o seguro.

As apólices de seguro cibernético ajudam a cobrir as perdas financeiras resultantes de eventos e incidentes cibernéticos e os custos associados à remediação, incluindo o pagamento de assistência jurídica, investigadores, atividades de gestão de comunicação institucional e reembolsos ao cliente. Muitas políticas de cibersegurança excluem problemas de segurança evitáveis causados por

humanos, como gestão de configuração deficiente ou manuseio incorreto e descuidado de ativos digitais.

O custo para melhorar os sistemas de tecnologia, incluindo reforço de segurança em sistemas ou aplicações, poderão estar na origem de exclusões das coberturas do seguro cibernético. A melhoria da segurança dos sistemas de tecnologia, incluindo reforço de segurança em sistemas ou aplicações, e violações, ou eventos cibernéticos preexistentes (ou anteriores), podem ser considerados como incidentes ocorridos antes da aquisição do seguro.

O seguro de cibersegurança é um setor novo e emergente e já está disponível em Portugal. Contudo, diferentemente das modalidades de seguro tradicionais, as seguradoras possuem dados limitados para formular modelos de risco e determinar as coberturas, taxas e prémios das apólices de seguro. Por esta razão, uma análise criteriosa deve ser feita antes de decidir pela aquisição.



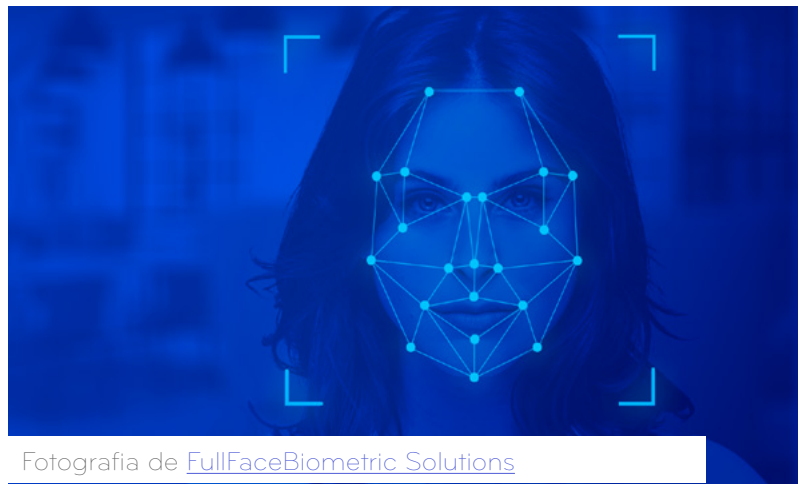
7. CASOS DE ESTUDOS

Exemplos de casos de estudo de startups ligadas à área da segurança digital, em que os seus negócios estão relacionados com serviços ao nível da Segurança, Fraude e Validações. Estes casos estão relacionados com startups portuguesas, europeias e brasileiras.

Fotografia de Mimi Thian disponível em Unsplash

Neste capítulo referem-se caso de estudo de startups ligadas à área da segurança digital, ao nível da Segurança, Fraude e Validações.

A FullFace Biometric Solutions (FullFace, 2021) tem como objetivo a identificação de pessoas. Com o aumento dos processos digitais, mecanismos de autenticação assentes em login e passwords não são a melhor forma de garantir a segurança da informação. Neste sentido, a FullFace Biometric Solutions está especializada na identificação de pessoas através de biometria facial em tempo real e no desenvolvimento de plataformas biométricas que envolvem a web e aplicações móveis.



Fotografia de FullFaceBiometric Solutions

Outros serviços e maior detalhe dos produtos e serviços da empresa podem ser encontrados aqui (FullFace, 2021).

Fotografia de ID Wall

A ID Wall (ID Wall, 2021) desenvolve vários serviços na área da segurança, onde se destaca a verificação de documentos OCR (*Optical Character Recognition* - reconhecimento ótico de caracteres) – em que o tipo de documento é identificado e os dados deste são extraídos de forma automática. A extração dos dados é realizada com recurso a diferentes tecnologias, e.g., o *Face Match*, que reconhece a imagem por comparação de uma *selfie* com a foto do documento; o *Background check*, que permite fazer a procura em mais de 200 fontes de dados da "Pessoa Física e Jurídica" (para agilizar o processo de onboarding digital de clientes e parceiros, considerando essencial a segurança do seu negócio); o *SDK Mobile*, que permite integrar soluções de forma rápida e segura, e a aprovação de clientes sem comprometer a segurança; A "Documentoscopia", que permite desencadear a análise de um documento, e verificar e confirmar se o documento foi produzido pela pessoa, organismo público ou privado (entidade que é suposta ter produzido o documento) e se sofreu alterações depois de finalizado, ou se foi "fabricado" indevidamente, por uma entidade terceira que procura assumir a identidade do autor; O *Professional Services*, integra serviços de consultoria em *onboarding* e validação de utilizadores.

A REDSTOUT (REDSTOUT, 2021) é uma empresa de tecnologia da informação, com sede em Lisboa, focada em soluções e serviços de cibersegurança de código aberto. A empresa nasceu da união de ideias e dos estudos de um grupo de alunos, como resultado do primeiro projeto RED (REDSTOUT Enterprise Defense) que tem o seu âmbito definido para suportar soluções de segurança de custo reduzido para Pequenas Empresas e Empresas Familiares.

Ao explorar as soluções de mercado, a empresa percebeu que os investimentos para acompanhar as legislações e ameaças (cada vez mais sofisticadas) representava um custo significativo para os pequenos negócios.

Os estudos desenvolvidos no âmbito do M.Sc. em Telecomunicações e Engenharia de Computação e Ph.D em Ciência e Tecnologia da Informação no ISCTE-IUL permitiram que o conhecimento fosse aplicado no desenvolvimento de produtos com base em software de código aberto para a proteção de dados. No seu início, a empresa contou com o apoio do Centro de Inovação e Empreendedorismo AUDAX-ISCTE (*Audax-ISCTE*, [2021]) na incubação de ideias e integração no ambiente de negócios em Portugal.

Para além dos sistemas, a empresa se estabeleceu como uma consultoria multidisciplinar com doutores e mestres em gestão, finanças, projectos e tecnologias que acumulam vasta experiência para apoiar qualquer tipo de negócio e prover processos e ferramentas mais modernos e seguros. Da estratégia à implementação e suporte, a REDSTOUT oferece experiência em segurança cibernética que vai além das soluções tradicionais de conformidade. Os serviços de consultoria REDSTOUT ajudam a reduzir o risco do seu negócio ao abordar as oportunidades e desafios únicos da sua organização. Os especialistas avaliam e orientam a correção das lacunas de conformidade da segurança da informação em todos os níveis da empresa, para ajudar a concentrar os recursos, tempo e orçamento de sua organização em áreas que agregam valor ou reduzem significativamente a exposição ao risco.

A REDSTOUT ampliou seus horizontes e está presente também em Angola (www.redstout.co.ao), a explorar um mercado repleto de oportunidades em segurança da informação.

O Noleak Behavior Recognition (NoLeak, 2021) é um sistema baseado em inteligência artificial para identificar ações e comportamentos suspeitos, captados através de sensores de câmaras RGB. O sistema correlaciona os eventos de várias câmaras (em tempo real), criando uma pontuação de risco para ambientes monitorizados. O sistema pode ser adaptado para detetar comportamentos humanos, em vários mercados e setores, na resolução de problemas.

A XLabs on security (XLAbs, 2021) é uma empresa, onde mais de 100 milhões de pessoas passam nos sistemas diariamente. Esta empresa tem quatro produtos principais:

Teste de intrusão

Utiliza várias técnicas para verificar as vulnerabilidades (ao nível de ataques direcionados, comprometendo a disponibilidade, integridade e confidencialidade das informações dos seus sistemas) e os riscos em redes internas ou mesmo na web.

Web Application Firewall

Esta aplicação protege as aplicações web contra as ameaças do Top 10 da OWASP 2021 (OWASP, 2021) e também a outras como acesso à base de dados, redireccionamentos, execução de comandos remotos, negação de serviço e inclusão de anúncios. Também deteta e bloqueia ameaças antes de atingirem os data centers, sem comprometer o desempenho das aplicações da empresa e responder a ataques direcionados com capacidade de identificar a localização.

Content Delivery Network

Esta ferramenta de desempenho distribui geograficamente o conteúdo da plataforma, implicando uma melhoria do desempenho e a segurança também.

O *Content Delivery Network* é uma rede de distribuição de informação que aumenta a velocidade através da utilização de múltiplos servidores que direcionam o conteúdo ao utilizador de acordo com a proximidade do servidor. A missão principal é encurtar a distância física entre o cliente e o servidor, melhorando a velocidade de renderização (processamento ou criação digital de uma imagem com pormenor e definição) e o desempenho do site.

Security Operations Center

É um produto que centraliza toda a operação de segurança. Este centro tem a capacidade de monitorizar os ambientes internos e externos ao nível das pessoas, processos e tecnologias para detetar incidentes de segurança, através da análise, deteção, prevenção e mitigação das vulnerabilidades nos sistemas e plataformas das organizações.

Em qualquer organização é necessário compreender os riscos e ameaças cibernéticas, a que organizações estão expostas, como primeiro passo para proteger os ativos de informação. É importante a adoção de uma abordagem pró-ativa e abrangente, para identificar o nível de risco e as vulnerabilidades antes que possam ser explorados. Os resultados da avaliação da segurança cibernética podem ser usados para determinar o orçamento para melhorar a segurança cibernética na organização, estimar os benefícios, e priorizar os investimentos.

A avaliação tem impacto ao nível de maior consciência e conhecimento da segurança cibernética (em todos os níveis da organização) e também impulsiona a responsabilidade e cria uma cultura de trabalho melhor. Ao estabelecer a segurança cibernética como uma prioridade, os colaboradores podem apoiar uns aos outros no uso seguro da tecnologia. Toda esta ação de avaliação tem resultados positivos ao nível dos processos, ferramentas e comportamentos para prevenir, resolver/mitigar rapidamente incidentes de segurança cibernética (evitando perda/roubo de dados) e, consequentemente o tempo de inatividade nos negócios e operações, perda de receita, exposição legal e publicidade negativa.

Glossário

- **Arquitetura de TI**

  A arquitetura de TI é a disciplina responsável por planear as tecnologias e transportar as necessidades de negócio para o ambiente tecnológico.

- **Ativos tecnológicos**

  Todos os componentes integrantes da infraestrutura de tecnologias da informação.

- **Cibercriminoso**

  Hacker não ético que ultrapassa os limites legais para recolher informações não autorizadas e executar transações eletrónicas de forma anónima.

- **CNCS**

  Centro Nacional de Cibersegurança.

- **CNPD**

  Comissão Nacional de Proteção de Dados.

- **Dado**

  Conjunto de caracteres ou símbolos que codificam informações.

- **Dados pessoais**

  Conjunto de dados que codificam informações pessoais.

- ***Endpoint***

  Pontos de acesso à informação numa rede de computadores, e.g., Notebooks, PCs, Tablets, telemóveis, entre outros.

- ***Framework***

  Modelo que tem por objetivo resolver problemas recorrentes.

- **GDPR**

  General Data Protection Regulation (Regulamento Geral de Proteção dos Dados).

- ***Hacker***

  Pessoa com conhecimentos informáticos capaz de explorar fragilidades e vulnerabilidades de segurança.

- **Informação pessoal**

  Qualquer informação que permita identificar uma pessoa singular.

- **IOT**

  Internet of Things (Internet das Coisas). Conceito que descreve a conectividade e troca de informações entre objetos físicos como carros, eletrodomésticos, equipamentos industriais, dotados da capacidade de enviar dados.

- **ISO**

  International Standardization Organization (Organização Internacional de Normalização ou Organização Internacional para Padronização).

- ***Malware***

  Pacote de software desenvolvido de forma a causar dano intencional.

- ***Phising***

  Técnica de recolha de informações e disseminação de malwares com a utilização do serviço de correio eletrónico.

- ***Ramsomware***

  Um grupo de malwares que sequestra dados e criptografa conteúdos, sendo geralmente utilizado para pedir resgate pelas informações roubadas.

- **RGPD**

  Regulamento Geral de Proteção dos Dados.

- **Risco Cibernético**

  Eventos tecnológicos que podem causar perdas no negócio causados por fragilidades e vulnerabilidades, no qual estão expostos os ativos tecnológicos.

- **SD**

  Segurança Digital.

- ***Shell***

  Interpretador de comando para o sistema operativo Linux.

- ***Sartup***

  Termo da língua inglesa que define uma "empresa emergente".

- **TIC**
  Tecnologias da Informação e Comunicação.

- ***Token***
  Chave eletrónica utilizada para identificar um utilizador, uma aplicação ou um endpoint.

- **Videoconferência**
  Plataforma para a realização de chamadas de voz e vídeo em grupo.

- **VPN**
  Virtual Private Network, ou rede privada, onde os dados são cifrados e enviados através de uma rede pública como a Internet.

Referências

Anderson, C. (2008), A Cauda Longa, Editora Campos.

Anderson, D., (2019), Storytelling: Manipulation of the Audience - How to Learn to Skyrocket Your Personal Brand and Online Business Using the Power of Social Media Marketing, Including Instagram, Facebook and YouTube, Independently Published.

(Audax—ISCTE, 2021), AUDAX-ISCTE, https://audax.iscte-iul.pt/, (Acedido Outubro de 2021).

(CNCS, 2020), CNCS - Relatório Sociedade 2020, https://www.cncs.gov.pt/pt/relatoriosociedade-2020/, (Acedido em Setembro de 2021).

(CNPD, 2021), Comissão Nacional de Proteção de Dados, https://www.cnpd.pt/, (Acedido em Setembro de 2021).

(IAPMEI, 2021), IAPMEI - Regulamento Geral de Proteção de Dados, https://www.iapmei.pt/PRODUTOS-E-SERVICOS/Assistencia-Tecnica-e-Formacao/Regime-Geral-de-Protecao-de-Dados.aspx, (Acedido em Setembro 2018).

(ISO 31000, 2021), ISO - ISO 31000—Risk management, https://www.iso.org/iso-31000-risk-management.html, (Acedido em Setembro 2021).

(ISO 27001, 2021) ISO - ISO/IEC 27001—Information security management, https://www.iso.org/isoiec-27001-information-security.html, (Acedido em Setembro de 2021).

(Keller, 2013), Cybersecurity Framework, NIST, https://www.nist.gov/cyberframework, (Acedido em Setembro de 2021).

(European Comission, 2021), O que são dados pessoais?, European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt, (Acedido em Setembro de 2021).

(INE, 2021), Portal do INE, https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=415621360&DESTAQUESmodo=2, (Acedido em Setembro de 2021).

(Regulamento, 2016), Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, Pub. L. No. 32016R0679, 119 OJ L (2016), http://data.europa.eu/eli/reg/2016/679/oj/por, (Acedido em Setembro de 2021).

(Ministros, 2019), Resolução do Conselho de Ministros 41/2018, Diário da República Eletrónico, de https://dre.pt/home/-/dre/114937034/details/maximized, (Acedido em Setembro de 2021).

- (Cybersecurity, 2021), The History of Cybersecurity, CompTIA's Future of Tech., https://www.futureoftech.org/cybersecurity/2-history-of-cybersecurity/, (Acedido em Setembro de 2021).
- (Setzer, 2021) Setzer V., Dado, Informação, Conhecimento e Competência https://www.ime.usp.br/%7Evwsetzer/dado-info.html, (Acedido em Setembro de 2021).
- (Data Classification, 2016), Data Classification – Why Is Data Classification Essential For All Businesses?, https://www.youtube.com/watch?v=fkHkmdgyYW8 (Acedido em Setembro de 2021).
- (Cibersegurança, 2020), Você sabe o que é a cibersegurança?, https://www.youtube.com/watch?v=CU2yQxzkvFg (Acedido em Outubro de 2021).
- (hackers, 2021), What is a hacker?, https://searchsecurity.techtarget.com/definition/hacker (Acedido em Outubro de 2021).
- (ISO 270001, 2013), ISO 27001 definition: What is ISO 27001?, https://www.itgovernance.co.uk/iso27001, (Acedido em Outubro de 2021)
- (malware, 20219), What is malware? Types and dangerous of malware, https://searchsecurity.techtarget.com/definition/malware (Acedido em Outubro 2021)
- (ransomware , 2021), How do ransomware attacks work?, https://searchsecurity.techtarget.com/definition/ransomware, (Acedido em Outubro de 2021)
- (phishing , 2021), How phishing works?, https://searchsecurity.techtarget.com/definition/phishing, (Acedido em Outubro de 2021)
- (Redstout, 2021), REDSTOUT ENTERPRISE DEFENSE, https://www.redstout.com, (Acedido em Outubro de 2021)
- (noleakdefence, 2021), Action/Behavior Recognition, https://www.noleakdefence.com, (Acedido em Outubro de 2021)
- (XLAbs, 2021), Produtos/soluções, https://www.on-security.com/pentest, (Acedido em Outubro de 2021)
- (OWASP, 2021), OWASP Top 10 - 2021, https://owasp.org/Top10/, (Acedido em Outubro de 2021)

Fotografias

Capa: Fotografia de Getty Images Signature disponível em Canva
Fotografia de Pickawood disponível em Unsplash
Fotografia de Camilo Jimenez disponível em Unsplash
Fotografia de Taylor Vick disponível em Unsplash
Fotografia de ricochet64. Créditos: Getty Images/iStockphoto.
Fotografia de Immo Wegmann disponível em Unsplash
Fotografia de Setyaki Irham disponível em Unsplash
Fotografia de Diego PH disponível em Unsplash
Fotografia de Mimi Thian disponível em Unsplash
Fotografia de ID Wall
Fotografia de FullFaceBiometric Solutions
Fotografia de Michael Geiger disponível em Unsplash
Fotografia de Luther.M.E. Bottrill disponível em Unsplash
Fotografia de Stephen Dawson disponível em Unsplash

Figuras

AUTORES
Marcio Santos
Cláudio Perim e
Pedro Sebastião

ENTIDADE PROMOTORA
IAPMEI, Agência para a Competitividade e Inovação, I.P.
Departamento de Empreendedorismo e Financiamento
Departamento de Capacitação e Valorização Empresarial

COORDENAÇÃO & REVISÃO
AUDAX – Centro de Inovação e Empreendedorismo do ISCTE-IUL
Pedro Sebastião
Luís Gonçalves

DESIGN GRÁFICO
I AM - The Creative House

DATA DE EDIÇÃO
Outubro de 2021

CONCEÇÃO
audax _iscte
IAPMEI

cofinanciado por

COMPETE 2020

PORTUGAL 2020

UNIÃO EUROPEIA

Fundo Social Europeu