CASTILLA Y LEÓN

“MANUAL DE CIBERSEGURANÇA NA EMPRESA”

Projeto COMPETIC

Apoio a empreendedores, trabalhadores independentes e microempresas no ambiente rural para criar e expandir os seus negócios aproveitando as oportunidades das TIC

Cámara Zamora

ipb Instituto Politécnico de Bragança

Diputación de Ávila

ACISAT

Interreg España - Portugal
Fondo Europeo de Desarrollo Regional
Fundo Europeu de Desenvolvimento Regional

UNIÓN EUROPEA
UNIÃO EUROPEIA

COMPETIC

Junta de Castilla y León

COMPETITIVIDAD

Este Manual foi preparado pela ENCLAVE FORMACIÓN para as oficinas realizadas no campo da consciencialização e formação em cibersegurança e confiança no âmbito digital, no âmbito do projeto COMPETIC que é desenvolvido no Programa Operacional de Cooperação Transfronteiriça Espanha - Portugal 2014- 2020, INTERREG VA Espanha - Portugal (POCTEP) no âmbito do Objetivo Temático 3: Melhorar a competitividade das pequenas e médias empresas e que é cofinanciado em 75% pelo Fundo Europeu de Desenvolvimento Regional (FEDER).

MAIS INFORMAÇÕES SOBRE O PROJETO COMPETIC E AS SUAS ATIVIDADES

Web: http://competic-poctep.com

E-mail: info@competic-poctep.com

ÍNDICE

CAPÍTULO 1. A IMPORTÂNCIA DA SEGURANÇA DAS TIC NAS PME.

1. CONCEITOS BÁSICOS SOBRE CIBERSEGURANÇA.

Hoje em dia utilizamos as novas tecnologias para desenvolver a nossa atividade profissional pelas possibilidades que nos oferecem:

- Somos mais produtivos.
- Chegamos a mercados que eram impensáveis há alguns anos atrás.
- Temos novos canais de comunicação, mais baratos, com clientes e fornecedores.

A tecnologia chegou já há anos à nossa vida pessoal e profissional e não se prevê que esta vá desaparecer, principalmente porque já não saberíamos viver nem trabalhar sem ela.

Através da Internet, desenvolvemos os nossos negócios, no entanto, **somente aqueles que se adaptarem a este novo ambiente de trabalho terão sucesso**, aproveitando-a ao máximo. Ao resto provavelmente acontecerá, como aos dinossauros, que acabarão por desaparecer.

Estamos no século em que a Tecnologia mudará radicalmente a maneira como vivemos e trabalhamos. Estamos continuamente a ouvir falar em termos como **BigData**, **MachineLearning**, **IA** (Inteligência artificial), **IoT** (Internet das Coisas), **Veículos Autônomos**, ... e **Cibersegurança**.

Se há algo que transcende todas as Tecnologias existentes e futuras, é a necessidade urgente de dotá-las de um nível de segurança que faça com que seu uso nos ajude, e não o contrário. As tecnologias, como sempre aconteceu, aparecerão e desaparecerão, no entanto, a necessidade de Cibersegurança permanecerá para sempre.

Por outro lado, e analisando o que aconteceu nos últimos 50 anos, a realidade é que não sabemos construir uma tecnologia segura. A princípio, o argumento era de que a tecnologia era projetada de acordo com as suas funcionalidades e ignorando as questões de segurança (porque naquela época não era considerada “necessária”). Contudo, a tecnologia que criamos hoje continua a ser afetada por inúmeras vulnerabilidades que podem implicar riscos para o seu utilizador pelo simples ato de usar. É também por esta assunção que é comum ser utilizada a expressão "a segurança informática a 100% não existe".

A validação dos argumentos acima mencionados pode ser feita através de consulta aos dados disponibilizados pelas organizações internacionais encarregadas de catalogar as vulnerabilidades relatadas pelos fabricantes de hardware e software, por exemplo, Mitre (https://cve.mitre.org).

De acordo com **CVE Details**, da Mitre, em 2017, as vulnerabilidades ultrapassaram de longe os registros dos anos anteriores, tendo sido reportadas mais de **14.700 vulnerabilidades** contra **6.447 em 2016**. O crescimento mais do que duplicou em comparação com os relatórios de 2016, existindo

um aumento de mais de 120% de um ano para o outro. E quando analisamos os valores para este ano de 2018, veremos que a progressão ainda é exponencial.

Por outro lado, a **cibercriminalidade** também está a aumentar de forma exponencial. E não é de estranhar pois o anonimato, oferecido pelo uso da tecnologia, para cometer crimes torna muito lucrativo assumir um risco muito baixo.

A máxima de "**ou te roubam o dinheiro ou te convertem em dinheiro**" é uma realidade para todos: grandes e pequenas empresas, administração pública, estado e indivíduos, ninguém está livre desta situação. Este é um aspeto de importância crucial num ambiente interligado e dependente da tecnologia.

Por esta razão, devemos tentar evitar a superexposição inerente ao uso da tecnologia, e isso será alcançado se nos soubermos proteger.

Cabe a todos alcançar um grau de segurança e confiança no ambiente digital que permita um desenvolvimento económico favorável para todos.

Mas... estas coisas não acontecem comigo?

Acabámos de dizer que nos afeta a todos. Além disso, as pequenas empresas e os trabalhadores independentes são um alvo mais fácil e mais barato de atacar pelos cibercriminosos, do que propriamente as grandes empresas e suas medidas de segurança caras e sofisticadas.

Mais da metade das empresas espanholas sofreram algum tipo de fraude económica nos últimos dois anos. Esta é uma das principais conclusões da pesquisa global sobre crimes económicos que a PwC elaborou, com base em 7.228 entrevistas em 123 países. Este valor coloca a Espanha acima da média mundial e acima dos principais países desenvolvidos.

Fonte: Relatório PwC 2018

Desde 2009, a percentagem de empresas espanholas vítimas de crimes económicos cresceu quase 20 pontos, passando de 35% para 54%. Um incremento que tem a ver com o aumento das Novas Tecnologias e, paradoxalmente, com o aumento dos controlos e uma maior consciencialização e perseguição deste tipo de fraude pelas empresas.

Apropriação indevida, corrupção e suborno, manipulação contabilística e ciberataques são os principais crimes económicos sofridos pelas empresas. E tudo aponta para que, nos próximos dois anos, a ciberfraude ganhará um peso significativo.

Para combater esta situação, as empresas espanholas estão a aumentar os orçamentos destinados a combater os ciberataques. Contudo, uma em cada dez empresas ainda não fez qualquer tipo de revisão ou avaliação de risco relacionado com cibersegurança.

Portanto, temos mais probabilidades de ser alvo de um ciberataque ou sofrer um incidente de segurança. Temos que estar cientes de que devemos proteger os nossos recursos, já que nos arriscamos a:

- Perder informação vital para o nosso negócio.
- Não ter os equipamentos, sistemas ou serviços disponíveis quando precisamos deles.
- Sofrer roubos de dinheiro.
- Ser alvo de extorsão por "sequestro" dos nossos computadores infetados por Ransomware ou problemas similares.

Em resumo, não podemos permitir que os nossos negócios e os nossos clientes possam sofrer qualquer dano em virtude de falta de cibersegurança.

Os riscos associados ao uso da tecnologia podem ser causados por várias causas:

- **Negligência ou erros**, numa percentagem muito alta das ocasiões.
- **Falta de consciencialização sobre** a importância da cibersegurança.

- **Ataques maliciosos,** externos ou internos.
- **Causas naturais** como incêndios, inundações, etc.

Tudo isto pode causar danos económicos e comprometer a continuidade do nosso negócio. Portanto, é importante que conheçamos os riscos inerentes ao uso das novas tecnologias, a fim de tentar minimizar o risco de sofrer um destes problemas.

A Internet, a nuvem e, mais recentemente, os desenvolvimentos do Big Data, Machine Learning e Internet das coisas (IoT) estão a causar uma mudança de paradigma:

- O mundo físico e o digital estão hiperconectados.
- Os utilizadores são um elemento ativo.
- A informação é processada, armazenada e transmitida sem restrições.
- Hoje geramos mais informações num único ano do que gerámos até 2011.
- Nas organizações temos ao nosso alcance mecanismos com os quais antes só poderíamos imaginar.

Este facto tem uma grande importância tanto para as empresas quanto para a sociedade. Os mercados e a economia tornaram-se globais e digitais. A cibersegurança é hoje indispensável.

Proteger a privacidade do consumidor, protegermo-nos contra ciberameaças (malware, fuga de dados, extorsão, roubo de identidade, ...), intencional ou não; e promover a segurança nos serviços é um fator essencial para o desenvolvimento da sociedade. Portanto, a legislação está a ser adaptada para que as sociedades possam tirar proveito desse novo paradigma sem reduzir direitos e liberdades.

Será complicado legislar contra novos ciberproblemas à mesma velocidade com que a tecnologia evolui. Contudo, a criação de legislação deve ser o mais célere possível visto que surgem constantemente novas tipologias de cibercrime, que ou são cometidos através de um suporte tecnológico ou são cometidos diretamente no ciberespaço, sem que até agora se possa atuar de forma efetiva na sua perseguição. As entidades reguladoras do Estado dizem-nos que, perante um ciberroubo, se o cibercriminoso não estiver fisicamente em Espanha ou se o bem roubado sair do país, praticamente não há nada a fazer.

Para termos uma ideia da importância do problema, os relatórios da Europool, de finais de 2016, referem o facto de já existirem países em que os cibercrimes excedem, em percentagem, os crimes tradicionais.

Lembrete. A cibersegurança da sua empresa é essencial e depende muito de si.

A maioria das grandes multinacionais está ciente dos riscos que assume ao usar tecnologia nos seus processos de produção e refletem esta consciência em investimentos, cada vez maiores, em cibersegurança.

No entanto, a perceção desse perigo em empresas menores é limitada e poucas têm entre as suas prioridades a proteção dos seus sistemas.

É preciso mudar o chip, porque para as PME, a informática sempre foi considerada uma despesa e não um investimento, de maneira que não é expectável que seja diferente em termos de cibersegurança. Precisamos de investir em tecnologia e segurança para garantir que os nossos negócios possam competir com as mesmas garantias que os restantes.

As PME empregam dez milhões de trabalhadores em Espanha e representam mais de 60% do PIB nacional, de acordo com dados do Ministério da Economia. A Confederação Espanhola de Pequenas e Médias Empresas pode-se orgulhar de que estas empresas compõem a quase totalidade do tecido empresarial do país. Por isto, não surpreende que 70% dos ataques informáticos ocorridos no ano passado - que são cerca de 125.000, segundo estimativas do Instituto Nacional de Cibersegurança - tiveram como alvo as PME.

O investimento de empresas com menos de 250 empregados em cibersegurança é inversamente proporcional ao risco de serem atacados.

As PME pensam que não são alvo de cibercriminosos, mas a realidade é que normalmente não são pessoas a atacar computadores, mas sim máquinas a atacar máquinas sendo, por consequência, os ataques altamente indiscriminados. Além disso, com centenas de milhares de sistemas, porque atacar o que está protegido?

Visto assim, parece atualmente que todos temos a obrigação de ser engenheiros informáticos para viver/trabalhar com segurança, mas não é assim. O que é necessário é um processo de consciencialização generalizada, como acontece com outros aspetos das nossas vidas que já interiorizámos, e é para isso mesmo que este curso se destina.

1.1. O VALOR DA INFORMAÇÃO NA EMPRESA.

Primeiro de tudo, devemos ter duas ideias claras:

- O primeiro é que **o que realmente tem valor no seu negócio é a informação** com a qual você trabalha e temos que identificar quais os ativos de informação que usamos e quais são as fontes de onde eles vêm.
  Ter que substituir equipamentos informáticos pode ser mais ou menos caro, no entanto, a maioria das empresas que perdem os seus dados não podem continuar a desenvolver a sua atividade normalmente, desaparecendo, num curto período de tempo, quando a recuperação da informação não é viável.

Alguns definem dados como o petróleo do século XXI.

- O segundo é que **devemos diferenciar os conceitos de Segurança Informática e de Segurança da Informação**.

Quando falamos sobre **Segurança informática** referimo-nos à segurança da infraestrutura tecnológica (equipamentos informáticos e de comunicações) que usamos para que o nosso negócio se possa desenvolver diariamente.

Quando falamos sobre **Segurança da Informação**, referimo-nos àquele ativo que indicámos como aquele que realmente tem valor, os dados, a informação.

A nossa empresa obtém informação de **múltiplas fontes (internas e externas)**, armazena-a **em vários suportes** (digital e não digital) e usa-a através de **múltiplos serviços** (documentos internos, correios eletrónicos, informação disponibilizada nas nossas páginas web, dados armazenados nas nossas bases de dados, ...).

Temos que ter em conta também o chamado **ciclo de vida da informação**, dado que o que hoje é importante para nós pode deixar de ser assim no futuro.

Para tudo o descrito acima, devemos realizar uma análise que nos permita:

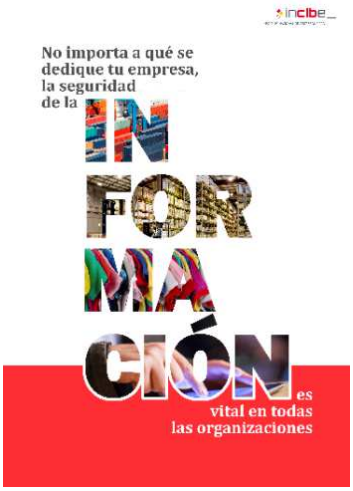
- Estruturar os nossos sistemas de informação.
- Classificar os nossos ativos de informação com base na sua atual e futura criticidade, de uma forma que nos permita identificar os procedimentos que devemos seguir para protegê-los e mantê-los em conformidade com as normativas vigentes.
- Definir uma série de mecanismos de controlo que nos permitam medir a eficácia das medidas de segurança que adotamos.

Por outro lado, a consciencialização e a educação, dos utilizadores devem ser feitas regularmente, envolvendo todos os participantes do programa de segurança que se está a definir. Nunca conseguiremos um resultado ótimo sem envolver todo o pessoal da empresa.

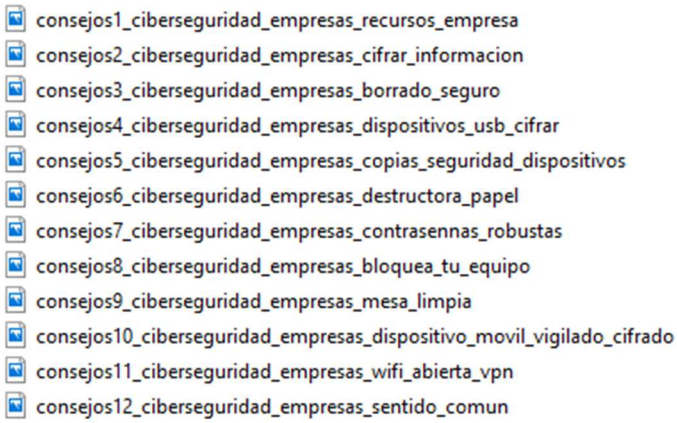
Instrumentos de conscientização:

- **INCIBE**: Desde https://www.incibe.es/protege-tu-empresa, é conveniente:
    - Acompanhar as publicações e formação setorial que é publicada recentemente pelo Instituto Nacional de Cibersegurança.

- Fazer download dos kits de consciencialização que encontramos na mesma página web onde teremos acesso a cartazes e trípticos que podemos colocar na empresa.



Publicar nas redes internas os conselhos que nos são oferecidos a partir dos kits de consciencialização para um uso seguro da tecnologia.



Estas são as etapas que o INCIBE propõe para a formação dos nossos trabalhadores, com base nos seus kits de consciencialização:

- **O Escritório de Segurança do Internauta**: (https://www.osi.es/es)
  Entidade que também depende do INCIBE e que fornece informação e suporte para evitar e solucionar os problemas de segurança que possam existir ao navegar na Internet.
  O seu objetivo é fortalecer a confiança no domínio digital por meio de formação em cibersegurança.
  Na OSI do INCIBE, trabalham para:

- Ajudar os utilizadores a realizar uma mudança positiva de comportamento em relação à adoção de bons hábitos de segurança.
- Torná-los conscientes da sua própria responsabilidade em relação à cibersegurança.
- Contribuir para minimizar o número e a gravidade das incidências de segurança sofridas pelo utilizador.

- **A Agência Espanhola de Proteção de Dados**: (https://www.aepd.es/)
  A AEPD é a autoridade encarregue de garantir a privacidade e a proteção dos dados dos cidadãos.
  O seu objetivo é, por um lado, incentivar os cidadãos a conhecer os seus direitos e as possibilidades que a Agência lhes oferece para exercê-los e, por outro, que os sujeitos tenham à sua disposição um instrumento ágil que lhes facilite a observância da norma.
  Todas as empresas, grandes e pequenas, públicas e privadas devem cumprir as normativas vigentes relacionadas com a proteção de dados dos seus trabalhadores, clientes, fornecedores, ... e mais ainda se eles pertencem a um dos grupos críticos: saúde, telecomunicações, ...
  Promover as formações direcionadas para a segurança de todos os nossos trabalhadores, permite reforçar as medidas e controlos implementados. As iniciativas do próprio INCIBE, ou esta mesma da Junta de Castilla y León, são contextos idóneos para começar no mundo da cibersegurança da empresa e conhecer as mudanças que estão a ocorrer constantemente: novas vulnerabilidades, novos riscos, novos tipos de ataques, novas formas de nos defendermos.

1.2. CIBERSEGURANÇA PARA AS PME.

Como deixámos antever, a gestão da segurança é o componente-chave para desenvolver um plano de proteção da informação que se adapte à idiossincrasia de cada empresa.

Sem gestão não há controlo que assegure eficientemente os dados da organização, nem a avaliação dos riscos a que estamos expostos.

Esta gestão deve ser entendida como um processo dinâmico:

1. Análise da situação.
2. Definição de um plano de controlo de segurança.
3. Implementação de medidas.
4. Avaliação de resultados.
5. Melhoria contínua. Isto implica recomeçar do ponto inicial.

Para isto definimos uma série de documentos que permitem que qualquer pessoa na organização tome consciência da segurança da informação e saiba o que é permitido e o que não é permitido no uso diário dos recursos. Além disso, indicam como devem ser realizadas certas tarefas que envolvem o uso da informação dentro da organização.

Um programa de Segurança da Informação deve contemplar medidas relacionadas com os colaboradores, a gestão e o uso da tecnologia. O funcionamento da organização está diretamente relacionado com os componentes informáticos e os sistemas de informação existentes, aumentando assim a sua criticidade com os resultados da empresa.

Por esta razão, um plano de segurança deve ter em conta a hierarquia da organização e ser funcional transversalmente na organização, contemplando em suma a **Integridade, Disponibilidade e Confidencialidade** da informação.

1.2.1. CLASSIFICAÇÃO DA INFORMAÇÃO.

Como acima indicado, precisamos de classificar a informação de acordo com sua criticidade e o impacto (negativo) que a sua perda teria. Isto permite determinar os recursos (económicos, humanos e outros), que é necessário destinar à proteção da referida informação. E quando falamos de segurança, nem tudo é resolvido com dinheiro.

Classificar a informação da organização é um componente-chave para a avaliação desta, tanto para os critérios de alocação de recursos, mencionados acima, tanto para a otimização das medidas de controlo a serem implementadas para cada tipo de informação. Quanto mais valiosa a informação para a empresa, mais recursos deveremos alocar para sua proteção.

Antes da classificação da informação, é necessário identificar todos os dados de valor para a organização. Para tal definimos uma série de documentos que, em conjunto, permitem que qualquer membro da organização ganhe consciência da importância da segurança da informação e saiba o que é permitido e o que não o é, no uso diário dos recursos. Além disso, estabelecem como devem ser realizadas certas tarefas que envolvem o uso da informação dentro da organização.

NÍVEIS DE CLASSIFICAÇÃO

Embora os critérios para catalogar a informação possam ser mais complexos e extensos, numa PME, podemos classificá-la em:

- **Confidencial**: para uso interno e de natureza restritiva. É uma informação valiosa que torna a empresa competitiva. Sua divulgação sem autorização pode afetar seriamente à organização. Por exemplo: um projeto de I & D, um código fonte, etc.
- **Privada**: Informação para uso interno da organização. É informação sensível e, em geral, de natureza privada. Sua divulgação pode afetar moderadamente a organização. Por exemplo: dados financeiros, dados médicos, dados pessoais, etc.
- **Pública**: Informação que não representa um impacto negativo na organização. Por exemplo: lista de endereços de correio dos empregados.

1.2.2. POLÍTICAS DE SEGURANÇA.

Uma Política de Segurança é uma declaração de intenções que cobre a segurança dos sistemas informáticos e fornece a base para definir e delimitar responsabilidades pelas várias ações técnicas e organizacionais que se pretendem executar.

É um documento de alcance global, válido para qualquer membro da empresa. É uma descrição geral dos fundamentos das medidas de segurança, o que se deseja proteger e como deve ser protegido.

Entre outras coisas, pode incluir:

- Objetivos e alcance.
- Classificação da Informação.
- Operações permitidas e recusadas com a informação.
- Acordos e contratos.

1.3. NORMAS E PADRÕES.

Os padrões são normas que afetam a interação dos utilizadores com os recursos da empresa e a informação que eles utilizam. Os padrões podem ser internos ou externos.

Entre os padrões internos mais comuns estão:

- O uso de equipamento informático por parte dos empregados.
- Software permitido (e proibido) no local de trabalho.
- Aceder ou não redes sociais particulares e outros serviços da web com conteúdo ilegal ou legal.
- Políticas de senhas e encriptação de informação, especialmente quando falamos sobre dispositivos móveis (smartphones, tablets ou portáteis) que tendem a sair da organização com informação sensível.

Os padrões externos geralmente são regulamentos ou leis que a empresa deve cumprir, que podem ser:

- De observância obrigatória ao ser afetada a empresa pela legislação vigente do país.
- Necessárias para poder trabalhar com parceiros que nos obrigam a adotar certos procedimentos de trabalho no âmbito do relacionamento entre entidades: padrões ISO, selo de cibersegurança,...

1.3.1. PROCEDIMENTOS.

Estas são ações documentadas que descrevem com precisão as tarefas a serem realizadas para cumprir com um objetivo. Permitem homogeneizar as tarefas que envolvem o uso de informação ou recursos informáticos da empresa, conseguindo minimizar os riscos que afetam a segurança dos mesmos.

Alguns exemplos dos procedimentos que podem ser usados numa PME são:

- Configuração de contas de correio.
- Configuração de VPNs (Redes Privadas Virtuais) para aceder a sistemas informáticos, desde o exterior, de forma segura.
- Configuração de cópias de segurança da informação e procedimentos de restauro.

2. USO SEGURO DE MEIOS DIGITAIS E NOVAS TECNOLOGIAS NA EMPRESA.

A transformação digital em que vivemos exige que se repense o uso que fazemos dos nossos locais de trabalho, do ambiente de trabalho em que realizamos o nosso trabalho, do espaço e a cultura do trabalho em si, e da gestão que fazemos do uso, correto ou incorreto, da tecnologia por parte dos nossos trabalhadores.

A tecnologia desempenha um papel essencial, que nos dá vantagens competitivas se a usarmos corretamente, mas que nos pode causar danos significativos se não a usarmos como devemos, ou se não implementarmos medidas de segurança razoáveis para protegê-la.

É fundamental assumir que as novas formas de trabalhar estão a desenhar um novo cenário na cultura de trabalho e na gestão de recursos. O espaço de trabalho foi redefinido, permitindo a mobilidade dos nossos trabalhadores de uma forma como nunca antes tinha acontecido. No entanto, este é um dos principais problemas que enfrentamos ao tentar proteger uma infraestrutura informática. Como se diz agora, **o perímetro foi perdido**, o que significa que as ferramentas e os protocolos de segurança que foram implementados há alguns anos, quando as informações não eram acessíveis desde o exterior da empresa, já não são úteis.

Como vem sendo dito ao longo deste curso, **a segurança da informação diz respeito à proteção da informação e dos sistemas de informação do acesso, uso, divulgação, interrupção ou destruição não autorizadas, independentemente do seu formato.**

Além disso, para protegê-la, poderemos aplicar medidas de segurança tanto físicas (videovigilância, biometria,...) como lógicas (senhas, encriptação,...).

Devemos assim perguntar a nós próprios o que aconteceria se essa informação caísse nas mãos de terceiros?

- Poderia perder vantagem competitiva? (informação sobre o meu negócio)
- Poderiam cometer um crime com essa informação? (fraude, roubo...)
- Estaria a revelar dados privados dos clientes ou a violar os direitos dos consumidores? Nestes casos, poderíamos ser sancionados. E não nos vai servir como desculpa o "eu não sabia". Devemos estar cientes de que a ignorância de uma lei não exime de ter que a cumprir.

E se perdermos ou destruirmos essa informação, como isso nos afetará?

- É informação crítica e necessária para o desenvolvimento do nosso negócio?
- O custo de recuperá-la ou gerá-la novamente seria muito alto?
- Poderia acontecer uma hipotética situação na qual não pudesse recuperar a informação?

A empresa deve começar a implementar medidas e controlos para proteger a informação e devemos ter em conta que o lugar onde devemos começar a implementar esses controlos técnicos está na **infraestrutura da organização**.

Chamamos infraestrutura de rede a todo o componente informático disponível para a realização do nosso trabalho. Não nos referimos apenas aos computadores dos utilizadores, mas também aos routers, aos *switches*, à cablagem de rede ou às redes wi-fi, às impressoras, aos dispositivos móveis, aos servidores, etc.

2.1. SEGURANÇA EM CAMADAS.

Como os riscos a que estamos expostos são diversos, devemos seguir um modelo de segurança em camadas, que consiste em organizar as medidas de segurança em diferentes níveis, garantindo que, se um nível for comprometido, o atacante tem que passar outra camada de segurança para danificar os sistemas.

2.2. COMUNICAÇÕES E NETWORKING.

Um dos principais problemas que as PME têm refere-se ao router fornecido pelo seu provedor de comunicações para dispor de serviço de acesso à Internet.

100% desses dispositivos são inicializados com a configuração por defeito de utilizador "administrador" do dispositivo e respetiva senha, sendo que muito poucos alteram posteriormente essa configuração.

Isto permite, de maneira muito simples, aceder ao dispositivo desde o exterior para poder alterar a configuração do mesmo. Por exemplo, um atacante pode alterar os servidores DNS aos quais o router faz consultas quando navegamos na Internet, redirecionando o tráfego para servidores ilegítimos. Desta forma, um atacante pode aceder ao tráfego das nossas comunicações externas, ficando a conhecer o nosso histórico de navegação e identificando os nossos "nomes de utilizador" e respetivas "senhas de acesso".

2.3. BYOD.

Bring Your Own Device é uma tendência cada vez mais generalizada, na qual as empresas permitem que os trabalhadores utilizem os seus dispositivos portáteis pessoais para realizar tarefas de trabalho e se ligarem à rede e aos recursos corporativos.

Sem um controlo básico deste tipo de dispositivos, temos uma lacuna de segurança muito importante na nossa organização. Um atacante poderia localizar um dos nossos trabalhadores, infetar o seu equipamento informático (se trabalhar desde casa, por exemplo), os seus dispositivos móveis (se se conectar desde o exterior para realizar o trabalho) ou os seus dispositivos de

armazenamento USB (levando e trazendo informação confidencial para a empresa), chegando a comprometer a nossa infraestrutura quando o trabalhador utiliza os seus dispositivos.

Se as nossas empresas ainda utilizam poucos mecanismos de segurança, os nossos trabalhadores, a título pessoal, costumam utilizar ainda menos.

2.4. ESQUEMA CLIENTE-SERVIDOR.

Um dos erros mais frequentes, particularmente nas PME, é a descentralização da informação. Entre as desvantagens de ter a informação distribuída em muitos equipamentos da rede (e particularmente em locais de trabalho) estão:

- **Problemas de disponibilidade**. Alguns utilizadores da rede podem precisar da informação e não saber onde encontrá-la ou como localizar quem sabe onde ela está armazenada.
- **Confidencialidade**. Alguma informação, não controlada, poderia ser acedida por pessoas não autorizadas para esse fim.
- **Dificuldade para fazer backup**. É extremamente complexo manter um backup completo da informação disponível em todos os postos de trabalho. Pode assim acontecer que não exista um backup de informação com valor.

2.5. POLÍTICAS DE ARMAZENAMENTO.

A existência de um servidor de ficheiros não significa que qualquer tipo de ficheiro precise de ser armazenado neste equipamento por qualquer tipo de pessoa. É por isso preciso definir as políticas de armazenamento para o servidor de ficheiros.

Em suma, devemos deixar bem claro e implementar as medidas para alcançá-lo, a que informação pode aceder cada utilizador.

2.6. REDUNDÂNCIA.

Quando todos os dados estão armazenados num único equipamento, normalmente um servidor de ficheiros, a criticidade desse servidor aumenta. Sendo essencial:

- Contar com um sistema de backup do mesmo.
- Usar sistemas de redundância que permitam a continuidade do negócio caso o disco rígido em que a informação está armazenada tenha alguma falha mecânica.

2.7. AMEAÇAS ATUAIS.

Desde a aparição dos vírus informáticos, na década de 1980, os códigos maliciosos (malware) evoluíram, encontrando novas características e métodos de propagação para afetar os utilizadores.

Por um lado, é importante poder classificá-los, para conhecer a diversidade de ameaças existentes, as suas características, as suas metodologias, as suas taxas de infeção, etc.

A classificação é importante para entender o que a ameaça do malware representa hoje. No entanto, devemos lembrar que todos estes tipos de malware têm um fator comum: prejudicar-nos. Portanto, a proteção contra ameaças deve abranger todos os tipos de códigos maliciosos, uma vez que qualquer um deles é um risco para os nossos interesses.

MALWARE

Malware é o acrónimo, em inglês, das palavras "**mal** icious "e" soft **ware**" (Em português, programa malicioso). Qualquer programa concebido com um objetivo prejudicial pode ser considerado como malware.

Malware é o termo principal usado para caracterizar todas as ameaças informáticas. Dentro desta categoria, já temos diferentes classificações mais específicas para as ditas ameaças, como trojans, worms, vírus informáticos, adware, spyware ou ransomware, entre outros. Também é muito comum a existência de malware que combina diferentes características de cada ameaça.

O malware já é considerado o maior problema de segurança do que levamos de século XXI, com um crescimento exponencial. O top 10 no ano de 2017 das famílias de malware foram: **WannaCry, Upatre, Cerber, Emotet, Locky, Petya, Ramnit, Fareit, PolyRansom e Terdot / Zloader.**

VÍRUS

Vírus informáticos precisam um anfitrião onde se hospedar. Isto pode variar, sendo um ficheiro (executável ou não), um setor de inicialização ou até mesmo a memória do computador. A sua origem data do início dos anos 80, sendo naquele tempo o único código malicioso existente (não existia ainda o conceito de malware). Aliás, no início, o malware era um tipo de vírus, enquanto os vírus agora são considerados um tipo de malware.

WORM

Um worm é um programa informático criado para produzir algum dano no sistema do utilizador e que possui duas características: ele age de forma transparente para o utilizador e tem a capacidade de se reproduzir.

Esta reprodução é fundamental para que um ataque seja bem-sucedido, pois será muito mais complicado erradicar a infeção de quase todos os nossos equipamentos do que apenas de um deles.

TROJAN

Os trojans (cavalos de troia) têm algumas semelhanças com os vírus informáticos, mas o seu funcionamento não é exatamente o mesmo. Enquanto um vírus é geralmente destrutivo, um trojan tenta passar despercebido enquanto acede aos nossos dispositivos com a intenção de executar ações ocultas tais como abrir uma "porta traseira" para que outros programas maliciosos possam aceder.

No entanto, um dos pontos comuns entre vários tipos de malware é que os trojans também se disfarçam de ficheiros legítimos. Fazem isto através de ficheiros executáveis cuja execução aparentemente não representa perigo, mas que, ao serem usados, começarão logo a funcionar ocultamente sem que o utilizador se aperceba.

ADWARE

Adware (acrónimo de "**ad** vertisement" - anúncio publicitário- e "soft **ware"**) é um programa malicioso, que é instalado no sistema sem que o utilizador saiba realmente o seu objetivo principal, que é fazer download e/ou exibir anúncios no ecrã da vítima.

Existindo ainda hoje, a realidade é que sua presença é muito menor do que era no passado. A grande diferença em relação ao adware de alguns anos atrás é que hoje ele está procurando outros propósitos, como a **mineração de criptomoedas**.

Normalmente, a atual infeção por adware está vinculada à visita de certas páginas da internet, à instalação de algumas extensões nos nossos navegadores sem verificar se são legítimas, ou ao download de aplicações nos nossos dispositivos mesmo estes tendo origem nas Stores oficiais da Microsoft, da Apple ou do Google.

SPYWARE

O spyware, também conhecido como software espião, é uma aplicação cujo objetivo é recolher informação do utilizador, sem o seu consentimento. Inicialmente, o spyware nasceu como um conjunto de aplicações incluídas em software gratuito, com o objetivo de gerar estatísticas sobre a atividade do utilizador no seu computador, a fim de determinar o seu perfil de navegação e interesses.

ROGUE

O rogue é um código malicioso que simula ser um programa de segurança, a fim de fazer com que o utilizador pague por uma aplicação nociva ou inexistente. É uma das técnicas que experimentou um rápido crescimento nos anos 2008 e 2009. Utiliza como ferramenta a geração de medo no utilizador, indicando falsos alertas sobre infeções e/ou problemas que o sistema poderia ter, conseguindo desta forma que o utilizador deseje instalar o produto falso.

RANSOMWARE

O ransomware é uma das ameaças de computador mais similares a um ataque sem meios tecnológicos: o sequestro, diretamente relacionado com moedas virtuais que, por inerência, não podem ser rastreadas na rede, e que são usadas para cobrança do resgate solicitado.

O ransomware é um código malicioso que, em geral, encripta a informação do computador e insere nele uma série de instruções para que o utilizador possa recuperar os seus ficheiros. A vítima, para obter a senha que liberta a informação do resgate, deve pagar ao atacante uma quantia em dinheiro, de acordo com as instruções que este comunique.

Algumas das técnicas de sequestro são as seguintes:

- Encriptação de ficheiros do disco rígido.
- Bloqueio de acesso a determinados ficheiros (geralmente documentos de origem administrativa).
- Bloqueio total de acesso ao sistema (antes do login ou bloqueio de ecrã quando o utilizar acede o sistema).

O INCIBE tem um serviço que ajuda as empresas que sofreram ataques de tipo ransomware.

OUTRAS AMEAÇAS

- **SPAM**

  Denomina-se Spam ao correio eletrónico não solicitado enviado por parte de um terceiro. Em espanhol, também é identificado como correio indesejado ou lixo eletrónico.

- **HOAX**

  Um hoax é um correio eletrónico distribuído num formato de cadeia, que visa fazer com que os leitores acreditem que algo falso é real. Ao contrário de outras ameaças, como phishing ou o scam; os “hoaxes” não têm fins lucrativos, pelo menos como intenção principal.

- **SCAM**

  Scam é o nome utilizado para fraudes através de meios tecnológicos. Com base na definição de fraude, o scam é descrito como o "crime consistente focado em causar prejuízo patrimonial a alguém por meio de fraude, com fim lucrativo e usando a tecnologia como meio".

- **PHISHING**

  O Phishing consiste no roubo de informação pessoal e/ou financeira do utilizador, através da falsificação de comunicações procedentes de uma entidade confiável.

  Desta forma, o utilizador acredita que está a inserir os seus dados num sítio que ele conhece quando, na realidade, estes dados são enviados diretamente para o atacante. Na sua forma clássica, o ataque começa com o envio de um correio eletrónico simulando a identidade de uma organização confiável, como, por exemplo, um banco ou uma reconhecida empresa.

As características de um e-mail de phishing são as seguintes:

- Uso de nomes de organizações com presença pública.
- O correio eletrónico do remetente simula ser da empresa em questão.
- O corpo do correio apresenta o logotipo da empresa que assina a mensagem.
- A mensagem insta o utilizador a reinserir algum tipo de informação que, na realidade, o suposto remetente já possui.
- A mensagem inclui um link.

O link é um componente importante. Quando o utilizador clica nele é redirecionado para um sítio web, onde poderá inserir a informação solicitada no correio eletrónico. Embora o texto mencione um endereço web válido, o mesmo pode apontar para qualquer outro sítio web; neste caso, para o sítio falsificado. Desta forma, o correio induz o utilizador a clicar nas ligações da mensagem.

3. AMEAÇAS, VULNERABILIDADES E RISCOS.

Saber identificar conceitos como ameaça, vulnerabilidade e risco, bem como um incidente pode afetar a sua empresa, permitirá que saiba se a sua empresa está em perigo.

Vulnerabilidade e ameaça são termos que muitas vezes são confundidos, por isso é necessário defini-los corretamente desde o início, como acontece com o risco:

Uma **vulnerabilidade** (em termos informáticos) é uma fraqueza ou falha num sistema de informação que coloca em risco a segurança da informação, permitindo que um atacante comprometa a integridade, a disponibilidade ou a confidencialidade da mesma. Portanto, precisaremos encontrá-las e corrigi-las quanto antes possível. Estes "buracos" podem ter origens diferentes, por exemplo: falhas de desenho, erros de configuração ou deficiências nos procedimentos.

Por outro lado, uma **ameaça** é uma qualquer ação que aproveita uma vulnerabilidade para atacar um sistema de informação, podendo assim ter um efeito negativo potencial em algum elemento dos nossos sistemas. As ameaças podem resultar de ataques (fraude, roubo, vírus), eventos físicos (incêndios, inundações) ou negligência e decisões institucionais (gestão incorreta de senhas, não uso de encriptação).

Do ponto de vista de uma organização, as ameaças tanto podem ser internas como externas.

Portanto, vulnerabilidades são as condições e características dos sistemas de uma organização que a tornam suscetível a ameaças. O problema é que, no mundo real, se houver uma vulnerabilidade, haverá sempre alguém que tentará tirar proveito da sua existência.

Uma vez que temos clara a diferença entre ameaça e vulnerabilidade, devemos saber que o **risco** é a probabilidade de ocorrência de um incidente de segurança, materializando uma ameaça e causando perdas ou danos. É medido assumindo que existe uma vulnerabilidade associada a uma determinada ameaça, tal como um cibercriminoso, um ataque de negação de serviço, um vírus... O risco depende da probabilidade da ameaça se materializar, aproveitando uma vulnerabilidade e causando dano ou impacto. O produto destes fatores representa o risco.

Associados ao risco, falamos sobre **análise de riscos** quando nos referimos ao uso sistemático da informação para identificar as fontes e calcular o risco, e de **gestão do risco** quando nos referimos às atividades coordenadas para dirigir e controlar uma organização em relação ao risco.

Esta análise/gestão levará à obtenção de uma imagem rigorosa dos riscos aos quais nossa empresa está exposta. Essas fases são as seguintes:

Dependendo da relevância dos riscos, podemos escolher:

- **Evitar o risco** eliminando a sua causa, por exemplo, quando for viável optar por não implementar uma atividade ou processo que possa implicar um risco.
- **Adotar medidas que atenuem o impacto ou a probabilidade de risco** através da implementação e monitorização de mecanismos de controlo.
- **Compartilhar ou transferir o risco** com terceiros através de seguros, contratos, etc.
- **Aceitar a existência do risco** e monitorizá-lo.

O tratamento do risco pressupõe benefícios claros para a "saúde" da cibersegurança da nossa empresa. Desta forma, manteremos a nossa informação confidencial, e a dos nossos clientes, protegidas contra a maioria das ameaças e vulnerabilidades detetadas (ou não), evitando roubos e fugas de informação.

Algumas das fontes mais comuns de ameaças no campo dos sistemas de informação são:

- **Malware ou código malicioso**: comentados na seção anterior.
- **Engenharia social**: são utilizadas técnicas de persuasão que aproveitam a boa vontade e a falta de cautela da vítima para obter informação sensível ou confidencial. Os dados assim obtidos são posteriormente usados para realizar outros tipos de ataques, ou para venda.

- **APT ou Ameaças Avançadas Persistentes** (Advanced Persistent Threats): são ataques coordenados direcionados contra uma empresa ou organização, que tentam roubar ou filtrar informação sem ser identificados. Costumam ter por base técnicas de engenharia social e são difíceis de detetar.
- **Botnets**: conjunto de equipamentos infetados que executam programas de forma automática e autónoma, permitindo que o criador da botnet controle os equipamentos infetados e os use para ataques mais sofisticados, como ataques DDoS.
- **Redes sociais**: o uso não controlado deste tipo de redes pode colocar em risco a reputação da empresa.
- **Serviços na nuvem**: uma empresa que contrata este tipo de serviço deve ter em conta que tem de exigir os mesmos critérios de segurança, que tem localmente nos seus sistemas, ao seu provedor de serviços. É preciso garantir que estes são contratados a empresas cuja capacidade de garantir níveis adequados de segurança esteja demonstrada, e garantir a assinatura de SLAs ou ANS (Acordos de Nível de Serviço) em que o nível de segurança de que a empresa precisa é definido.
- Alguns incidentes podem implicar **problemas legais** que podem comportar sanções económicas e danos à reputação e imagem da empresa. Portanto, é importante conhecer os riscos, medi-los e avaliá-los para evitar, na medida do possível, os incidentes, implantando as medidas de segurança apropriadas.

4. BOAS PRÁTICAS.

4.1. SEGURANÇA FÍSICA.

A segurança física dos sistemas informáticos consiste na aplicação de barreiras físicas e procedimentos de controlo, como medidas de prevenção e deteção, destinadas a proteger fisicamente qualquer recurso do sistema.

Este fato é de vital importância nos equipamentos (portáteis, tablets ou smartphones) que no âmbito da atividade empresarial tendem a ser móveis e a sair das instalações físicas da empresa.

Dependendo do ambiente e dos sistemas a serem protegidos, esta segurança será mais ou menos importante e restritiva, embora seja preferível pecar por excesso de zelo: exposição mínima / privilégio mínimo.

Por outro lado, temos que interiorizar o conceito de **resiliência**, que se refere à capacidade de uma empresa para se adaptar e continuar com as suas funções e o seu trabalho em situações de risco. Como agir e como **gerir a situação de forma eficiente** afetando, o mínimo possível, o desempenho geral da empresa. Ou, em outras palavras, uma empresa é resiliente se implementou as medidas corretas para restabelecer qualquer serviço no menor tempo possível quando ocorreu um incidente de segurança / cibersegurança.

Em seguida, destacaremos alguns dos problemas de segurança física que podemos enfrentar e as medidas que podemos tomar para minimizar o seu impacto.

Devemos realizar uma monitorização contínua da nossa infraestrutura para conhecer, em tempo real, a situação de risco em que nos encontramos e, além disso, é preciso promover uma cultura de segurança empresarial educando todos os membros da empresa sobre as boas práticas para evitar riscos e para saber como agir em caso de incidente.

PROTEÇÃO DO HARDWARE

Problemas que enfrentamos:

- Acesso físico.
- Desastres naturais.
- Alterações do ambiente.
- Acesso ao próprio dispositivo informático.0

ACESSO FÍSICO

Se alguém que deseje atacar um sistema tiver acesso físico a ele, todo o resto de medidas de segurança implementadas tornam-se inúteis. Isto não seria um grande problema se protegêssemos o que normalmente não protegemos corretamente: nem os espaços em que localizamos os nossos equipamentos informáticos nem o acesso aos mesmos.

Quanto a proteger o espaço em que temos os nossos equipamentos informáticos, teremos que implementar mecanismos de **prevenção** (controlo de acesso aos recursos) e de **deteção** (se um mecanismo de prevenção falhar ou não existir, devemos pelo menos detetar os acessos não autorizados o mais rapidamente possível).

Para a **prevenção** existem muitas possibilidades que permitem registar quem acede a que recursos e a que horas:

- Sistemas biométricos: analisadores de retina, leitores de impressões digitais, ...
- Cartões inteligentes.
- CCTVs.
- ...

Em muitos casos, é suficiente controlar o acesso às salas e fechar sempre à chave os escritórios ou salas onde há equipamentos informáticos e não ter cabladas as tomadas de rede que estejam acessíveis.

DESASTRES NATURAIS

Além dos possíveis problemas causados por ataques feitos por pessoas, é importante ter em conta que também os *desastres naturais* podem ter consequências muito graves, especialmente se não os contemplarmos na nossa política de segurança e na sua implementação.

Alguns desastres naturais a considerar:

- Terramotos e vibrações.
- Trovoadas.
- Inundações e humidade.
- Incêndios e fumos.

Os terramotos são o desastre natural menos provável num país como a Espanha, por isso não serão feitos grandes investimentos em preveni-los, contudo, se fôssemos abrir um escritório no Japão, a situação mudaria drasticamente. Além disso, existem várias coisas que podem ser feitas sem um custo elevado e que são úteis para evitar problemas causados por pequenas vibrações:

- Não colocar os equipamentos em locais altos para evitar quedas.
- Não colocar elementos móveis sobre os equipamentos para evitar que caiam sobre estes.
- Afastar os equipamentos das janelas para evitar que caiam por elas ou que objetos lançados do exterior os danifiquem.
- Usar fixações para elementos críticos.
- Colocar os equipamentos sobre plataformas de borracha para absorver as vibrações.

Outro desastre natural importante são as trovoadas, especialmente frequentes no verão, que geram subidas súbitas de tensão muito superiores às que possam gerar um problema na rede elétrica. Além da proteção mediante o uso de tomadas de terra, podemos usar UPS que mantenham acesso aos equipamentos críticos em caso de perda de corrente. Nesses casos, é aconselhável desligar os equipamentos quando houver uma tempestade.

Em ambientes normais, recomenda-se que haja um certo grau de humidade, já que se o ambiente estiver extremamente seco há muita eletricidade estática. No entanto, também não interessa ter um nível de humidade muito alto, dado que pode ocorrer condensação nos circuitos integrados que origine um curto-circuito. Em geral, não é preciso usar qualquer tipo de aparelho para controlar a humidade, mas convém ter alarmes que nos avisem quando houver níveis anómalos.

Outro tema diferente são as inundações, uma vez que se um equipamento (servidores, routers ou switches, sistemas de armazenamento e backup de dados, ...) entrar em contacto com a água fica automaticamente inutilizado, bem pelo próprio líquido como pelos curtos-circuitos gerados pelos sistemas eletrónicos. Contra elas, podemos instalar sistemas de deteção que desliguem os sistemas se a água for detetada e desliguem a energia assim que estes estiverem desligados. Deve indicar.se quais os equipamentos que devem estar acima do sistema de deteção de água, senão quando se tentar parar, já estará molhado.

Por último, mencionaremos o fogo e os fumos, provenientes em geral de incêndios dos equipamentos devido à sobrecarga elétrica. Contra eles usaremos sistemas de extinção, que são atualmente mais ou menos inócuos e permitirão evitar males maiores. Além do fogo, o fumo também é prejudicial para os equipamentos (até mesmo o do tabaco), já que é um abrasivo que ataca todos os componentes, sendo por isso recomendável mantê-lo o mais afastado possível dos equipamentos.

ALTERAÇÕES DO AMBIENTE

No nosso ambiente de trabalho existem fatores que podem sofrer variações que afetam os nossos sistemas e que precisamos de conhecer e de tentar controlar.

Será necessário contemplar problemas que podem afetar o regime de funcionamento habitual das máquinas, tais como a alimentação elétrica, o ruído elétrico (produzido pelos equipamentos) ou as mudanças bruscas de temperatura.

ELETRICIDADE

Talvez os problemas mais frequentes decorrentes do ambiente de trabalho sejam aqueles relacionados com o sistema elétrico que alimenta os equipamentos; curtos-circuitos, picos de tensão, cortes de fluxo...

Como indicámos anteriormente, para corrigir problemas relativos a picos de tensão, poderemos instalar tomadas de terra ou filtros reguladores de tensão UPSs (Fonte de Alimentação Ininterrupta).

Por último, indicar que, além dos problemas do sistema elétrico, também nos devemos preocupar com a corrente estática, que pode danificar os equipamentos. Para evitar este tipo de problemas, podem ser utilizados sprays antiestáticos ou ionizadores, ter cuidado para não tocar em componentes metálicos, e evitar que o ambiente esteja excessivamente seco, etc.

Ruído elétrico

O ruído elétrico tende a ser gerado por motores ou maquinaria, mas também pode ser gerado por computadores ou por uma multiplicidade de aparelhos, sendo transmitido através do espaço ou de linhas elétricas próximas à nossa instalação.

Para evitar os problemas que o ruído elétrico pode causar, não devemos colocar o *hardware* perto dos elementos que podem causar ruído. Caso seja necessário, podemos instalar filtros ou isolar as caixas dos equipamentos.

Temperaturas extremas

Não é preciso ser um génio para perceber que temperaturas extremas, seja calor excessivo ou frio intenso, prejudicam gravemente todos os equipamentos. Em geral, recomenda-se que os equipamentos operem entre 10 e 32 graus Celsius. Para controlar a temperatura devemos usar aparelhos de ar condicionado.

Proteção dos dados

Além de proteger o hardware*, a* nossa política de segurança deve incluir medidas de proteção de dados, dado que, na realidade, a maioria dos ataques visam a obtenção de informação, não a destruição do meio físico que a contém.

Suportes não eletrónicos

Outros elementos importantes na proteção da informação são os elementos não eletrónicos que são usados para a sua transmissão, principalmente o papel. É importante que nas organizações que tratam informação confidencial sejam controlados os sistemas que permitem exportá-la tanto em formato eletrónico como em formato não eletrónico (impressoras, plotters, fax, ...).

Qualquer dispositivo através do qual a informação possa sair do nosso sistema deve estar localizado num local de acesso restrito; também é conveniente que o local onde os utilizadores armazenam os documentos criados nesses dispositivos seja de acesso restrito.

Além disso, é aconselhável ter trituradoras de papel para destruir todos os papéis ou documentos que se queira destruir, uma vez que evitaremos que um possível atacante possa obter informação procurando no nosso lixo.

Acesso ao próprio dispositivo informático

Devemo-nos acostumar a ativar e utilizar a utilização de uma senha na BIOS em todos os equipamentos e dispositivos informáticos, sendo esta opção ainda mais relevante naqueles que tiramos da empresa.

Além disso, devemos usar senhas seguras para aceder ao sistema operativo, obrigando a mudar esta mesma senha com uma periodicidade pré-estabelecida.

Finalmente, devemos encriptar os discos rígidos dos dispositivos, para tornar as informações ilegíveis no caso destes caírem nas mãos erradas. Em tablets e smartphones, podemos configurar a eliminação remota do dispositivo no caso deste ter sido roubado ou de tê-lo perdido.

4.2. CÓPIAS DE SEGURANÇA.

Já comentámos que o que realmente tem valor na empresa é a informação e por isso é necessário existir um procedimento para a realização de cópias de segurança e outro, paralelo, de restauração de cópias.

O sistema de cópia de segurança que implementaremos dependerá da informação que precisamos de proteger e do local onde esta está armazenada. As empresas que virtualizarem os seus sistemas não utilizarão os mesmos procedimentos. Sendo assim, estes procedimentos são importantes para quem possui, por exemplo, sistemas gestores de bases de dados, ou sistemas operativos Windows ou Linux, ...

Por esta razão, em primeiro lugar devemos realizar uma auditoria que nos permita escolher a solução que melhor se adapte às nossas necessidades.

Por outro lado, devemos combinar as cópias de segurança que armazenamos "no local", nos nossos escritórios, com cópias de segurança na nuvem. Atualmente, os custos destes serviços são viáveis e permitem ter, fora da empresa, uma cópia de segurança que nos permita continuar com a atividade em caso de uma catástrofe.

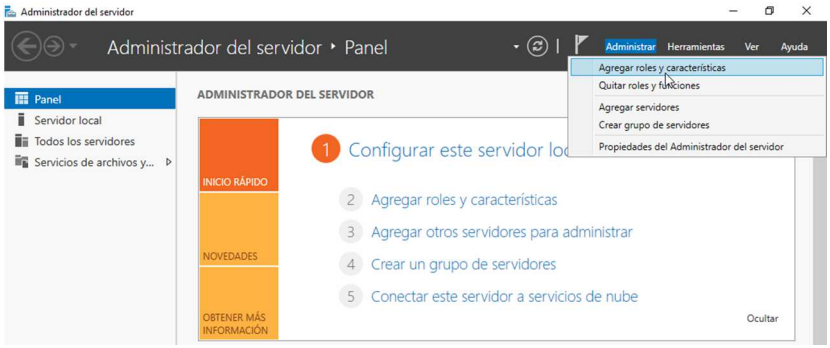
Embora sejam situações extremas, lembre-se do acontecido nos ataques de 11 de setembro nos Estados Unidos ou no incêndio do prédio Windsor em Madrid. As empresas que tinham escritórios nesses prédios e não tinham cópias de segurança on-line, não puderam continuar com suas atividades porque não conseguiram recuperar a informação, embora tivessem cópias de segurança nos seus escritórios.

Para ambientes com servidores Windows Server, podemos usar a ferramenta de cópia de segurança integrada no próprio sistema.

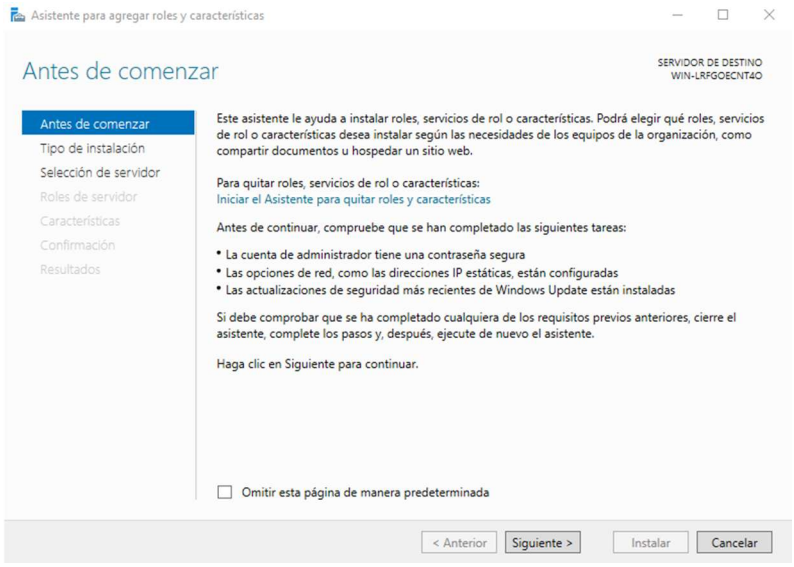
Através desta ferramenta podemos:

- Fazer backup completo do Servidor.
- Fazer backup das unidades de armazenamento de dados, localizadas no próprio servidor ou em unidades de rede.
- Programar a periodicidade das cópias de backup: diariamente, semanalmente, ..., nas horas do dia em que nenhuma atividade é desenvolvida.
- Combinar essa periodicidade com a realização de backups completos ou incrementais.

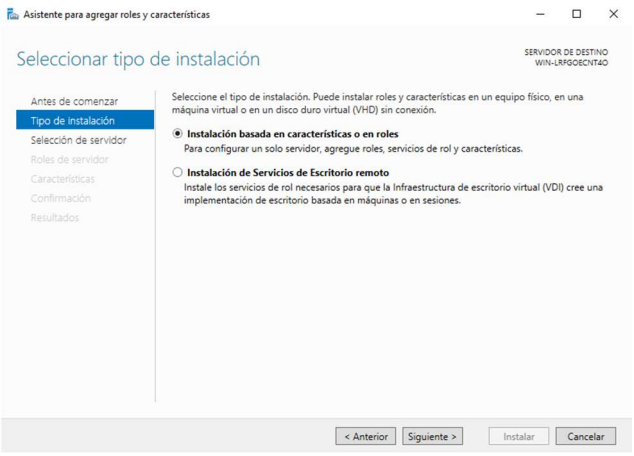
Podemos aceder a esta ferramenta através do menu “Ferramentas” no painel de Administrador do Servidor.



Em seguida, seguiremos o assistente de agregação de funções e características:

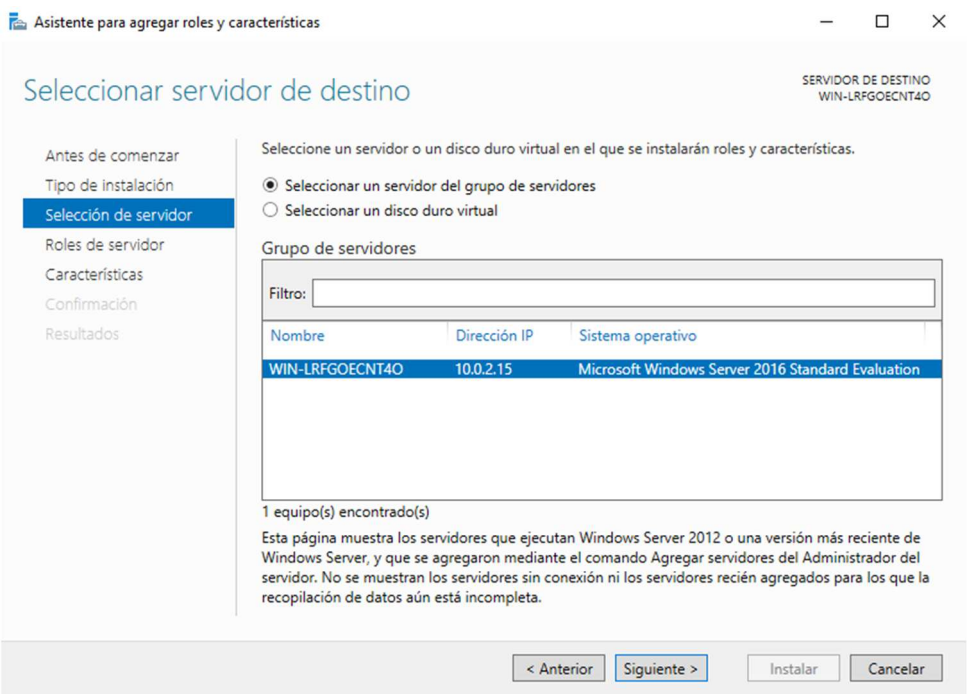


Neste momento podemos visualizar uma descrição do que podemos fazer através do assistente. Escolhemos “Seguinte”, e em seguida, escolhemos a opção que vem por defeito:

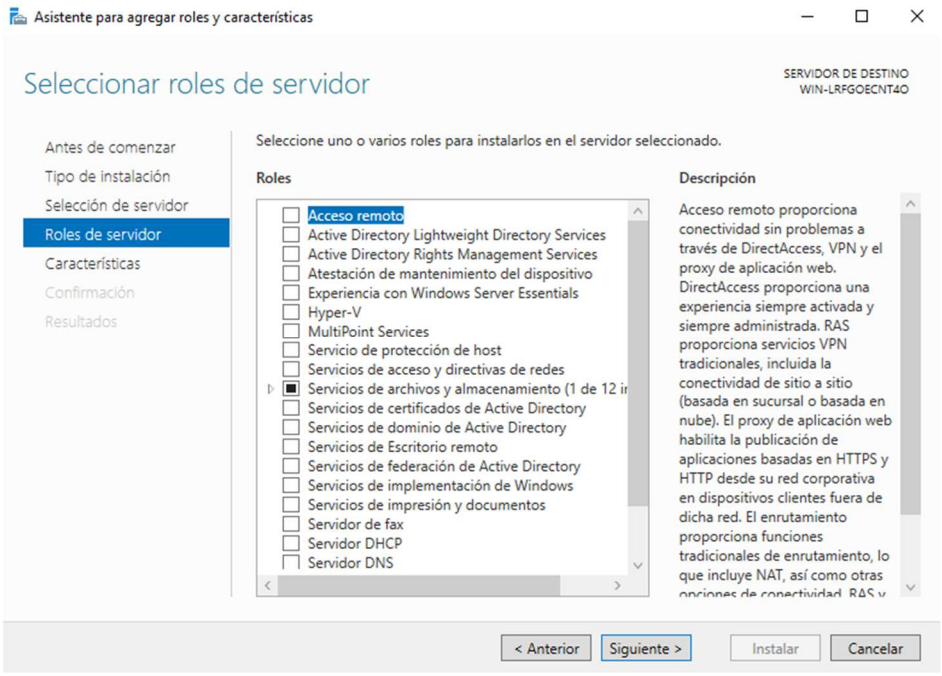


Com esta opção, estamos a dizer que queremos fazer uma instalação para aceder localmente ao serviço no servidor em que o instalarmos.

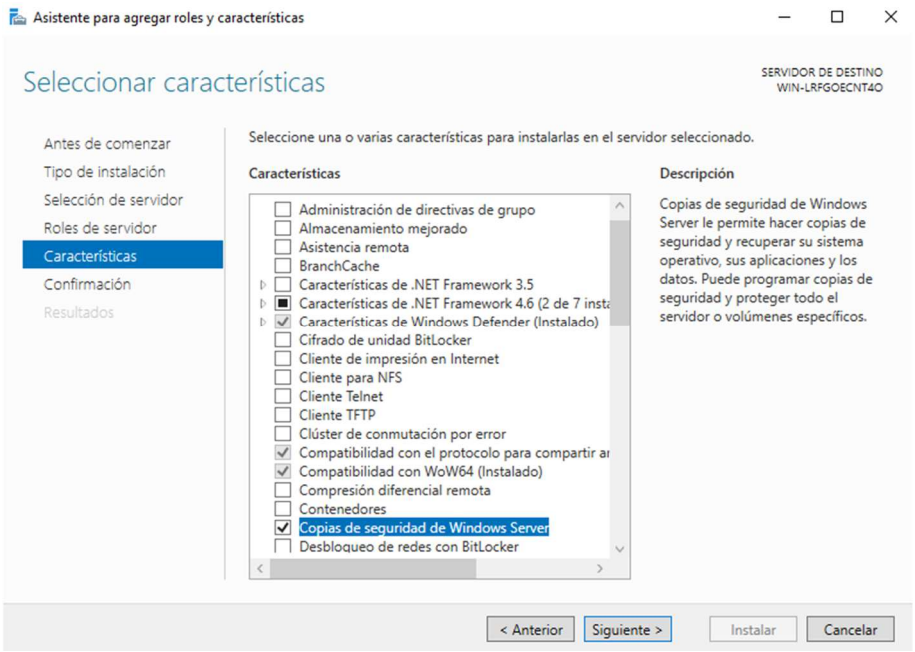
Em seguida, indicamos em qual servidor queremos instalar o serviço. Se tivermos apenas um, como no exemplo, basta clicar em “Seguinte”:



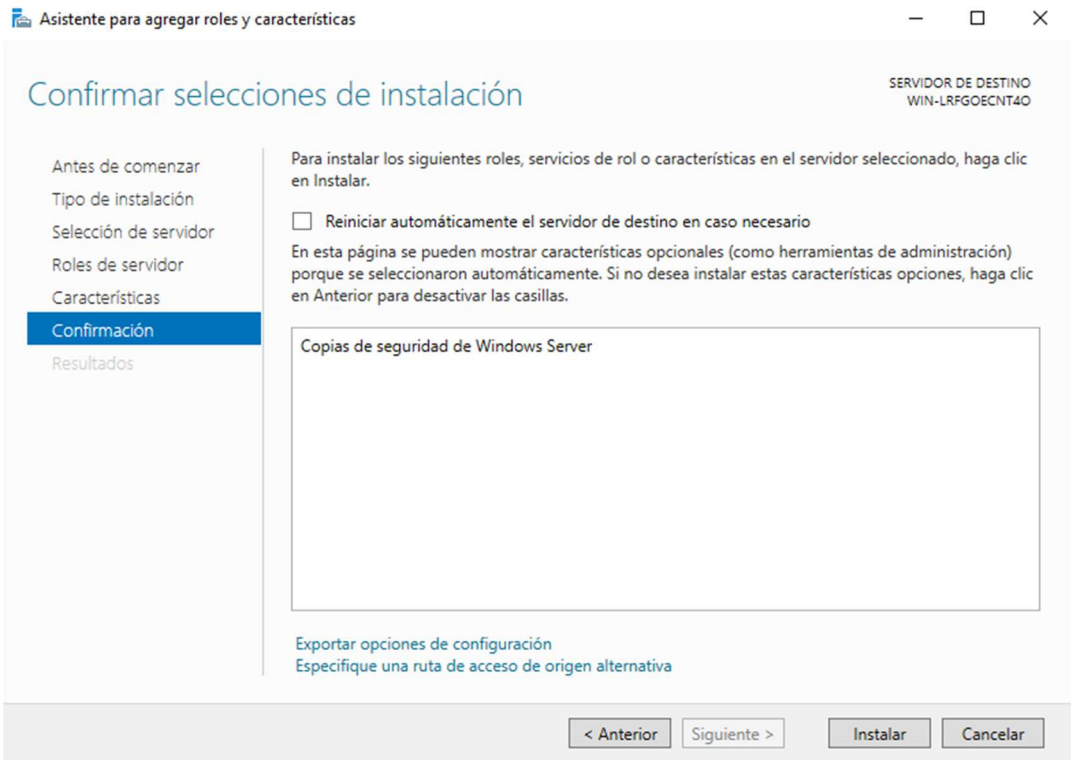
Uma vez na seção “Funções do Servidor”, clicaremos em “Seguinte” sem selecionar nenhuma opção porque a ferramenta de backup não é uma “função”, mas sim uma “característica”:



Uma vez na seção “Características”, escolhemos “Cópias de segurança do Windows Server” e clicamos em “Seguinte”:

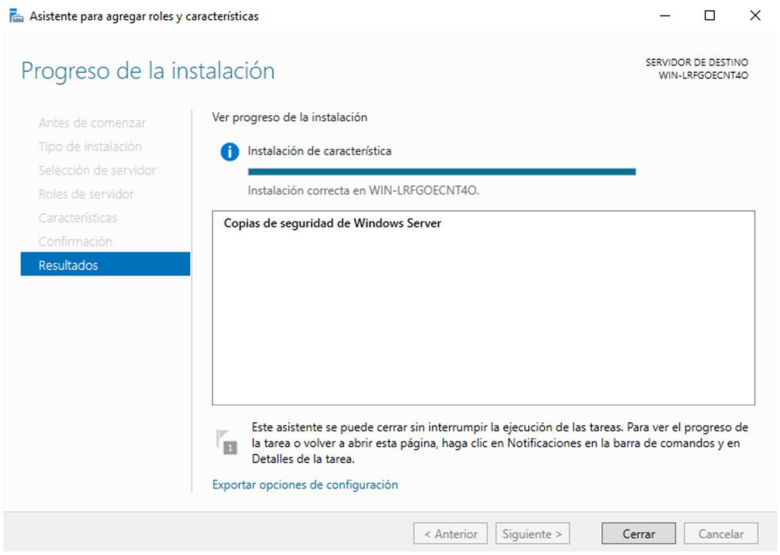


Neste momento, podemos indicar se permitimos ou não reiniciar automaticamente o servidor caso a instalação o exija, e clicamos em “Instalar”:

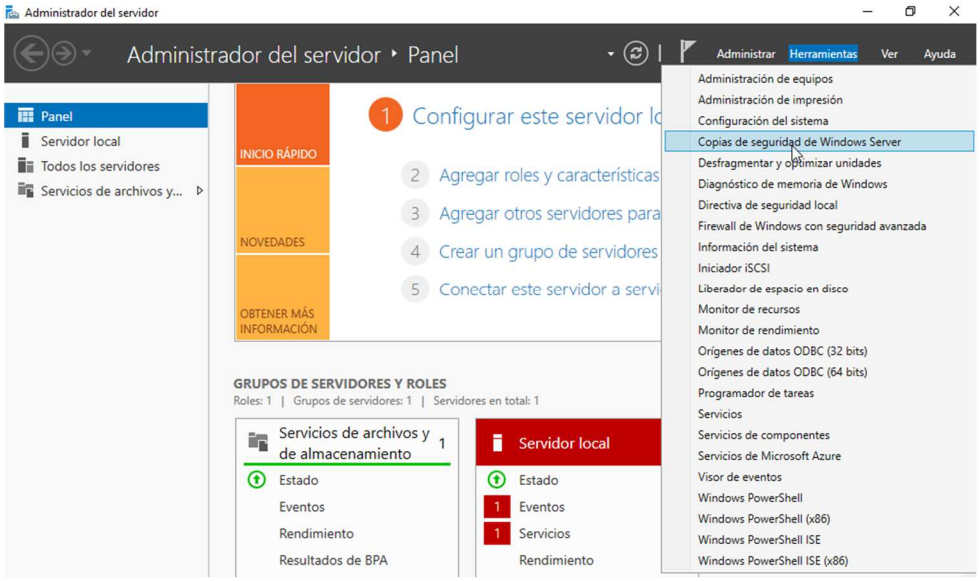


O processo de instalação é rápido e podemos até deixá-lo em segundo plano clicando em fechar.

Quando finalizar, irá surgir uma janela indicando que o processo foi executado corretamente:



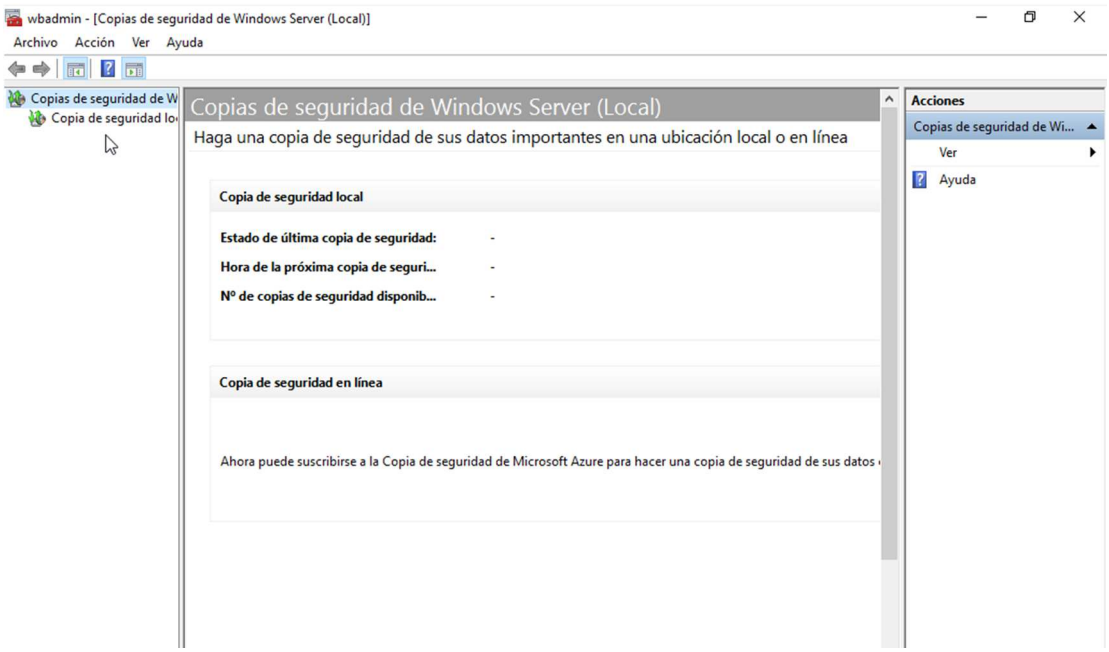
Uma vez instalada a ferramenta de backup, podemos aceder-lhe através das Ferramentas do Administrador do Servidor:



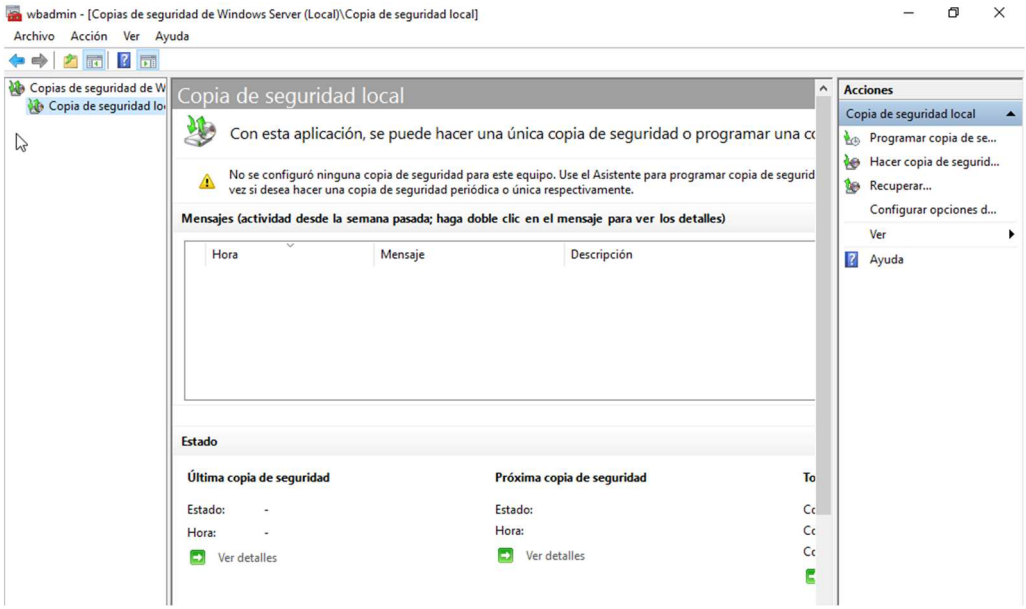
Como pode observar, até agora, o processo de instalação não é complexo e não requer grandes conhecimentos informáticos.

De seguida veremos como podemos usar o referido serviço e observaremos que o seu uso também é simples e não requer grandes conhecimentos.

Assim que clicamos na Ferramenta de Segurança do Windows Server, encontramos a seguinte interface:



Clicando em “Cópia de Segurança Local” o serviço irá procurar cópias de segurança já realizadas para nos mostrar. Neste primeiro momento dir-nos-á que nenhuma cópia foi ainda configurada:



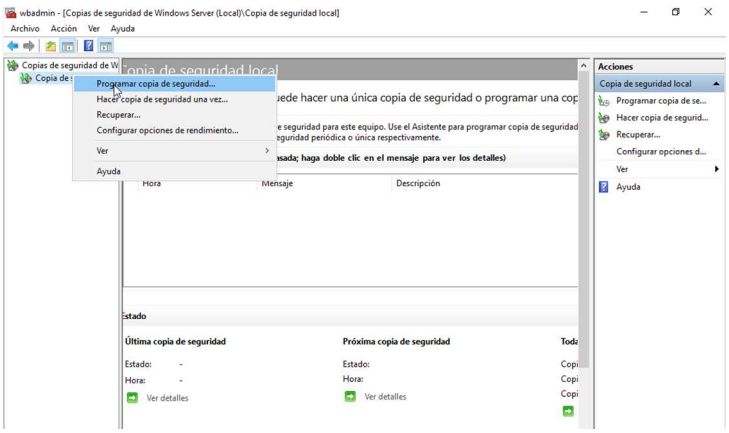
Estamos agora prontos para configurar a nossa primeira cópia de segurança, mas, antes de tudo, devemos fazer uma análise sobre qual a informação que precisa de ser incluída numa cópia de segurança e com que periodicidade. Por outro lado, também podemos fazer uma cópia de segurança completa do nosso servidor, o que nos permitirá recuperá-lo muito rapidamente, caso tenha sido comprometido.

Tenha em conta que nosso principal objetivo é ser resilientes, ou seja, devemos ser capazes de reiniciar um serviço que tenha “caído” no menor tempo possível, para que o impacto da paragem seja mínimo.

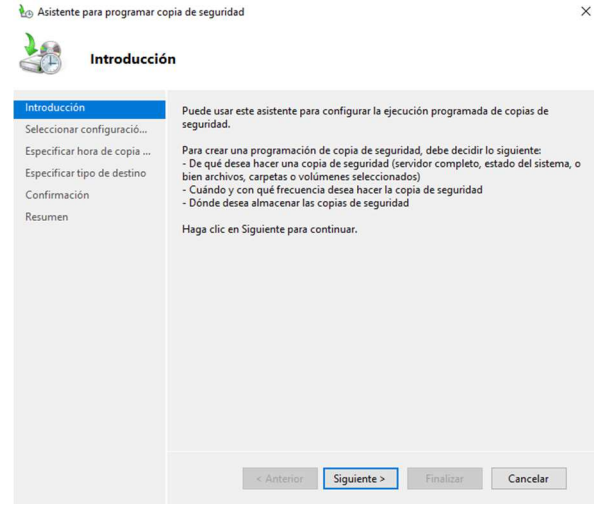
Neste momento, devemos indicar se queremos realizar uma cópia de segurança imediatamente ou se queremos programar um processo que seja repetido periodicamente. Independentemente do facto de que num momento específico me interesse realizar uma cópia de segurança pontual, devemos programar cópias periódicas.

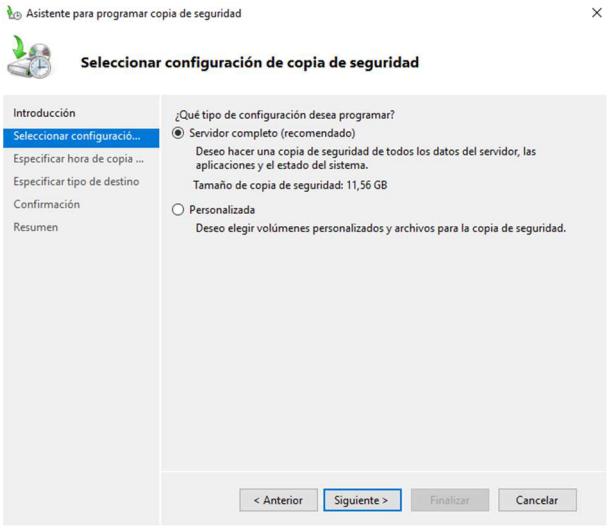
Essas cópias devem ser realizadas fora do horário de atividade da empresa, uma vez que tendem a causar um grande impacto sobre o desempenho do servidor e também porque não vão incluir os ficheiros que estiverem a ser usados no momento em que a cópia estiver a ser realizada.

Vamos ver como podemos programar uma cópia de segurança. Clicamos com o botão direito do rato sobre “Cópia de Segurança Local”:



Em seguida, aparece o assistente que devemos seguir:



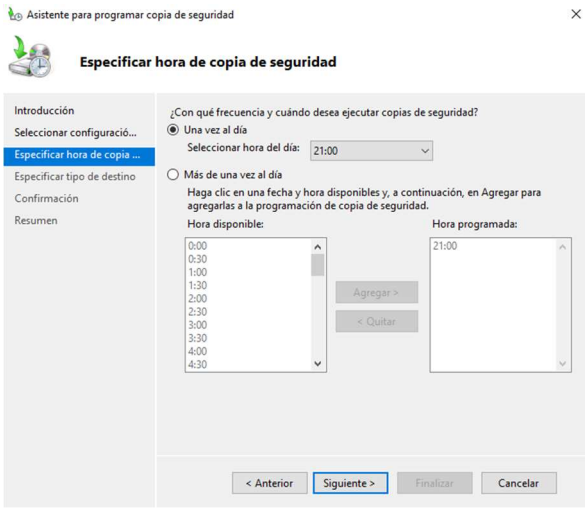


Neste ecrã, é-nos dito os detalhes que temos de considerar antes de continuar.

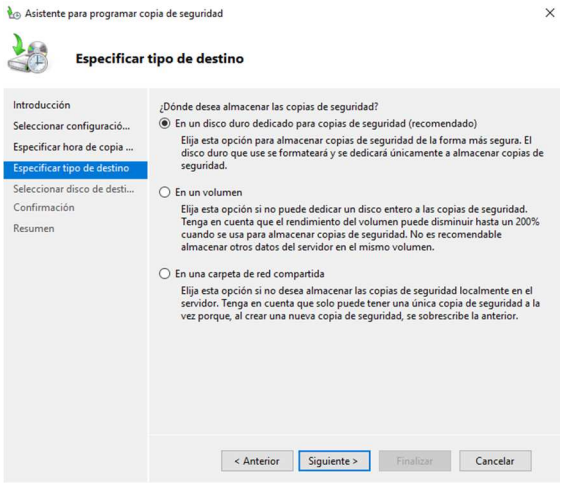
Clicamos em “Seguinte” e indicamos se queremos realizar uma cópia completa do servidor ou selecionamos o que queremos incluir na cópia:

Devemos ter dois tipos de cópias de segurança. Uma periódica completa, diariamente, que como já foi indicado irá permitir restaurar o sistema num curto espaço de tempo, quando tivermos um incidente grave, e devemos realizar outra cópia só da informação. Esta última deverá ser realizada por meio de duas cópias de segurança independentes: uma semanal completa e outra diária incremental, isto permitirá que seja realizada mais rapidamente, guardando somente a informação modificada desde a última cópia de segurança.

Neste momento, veremos como realizamos uma cópia completa do servidor clicando em “Seguinte”. Aparecerá o seguinte ecrã do assistente:



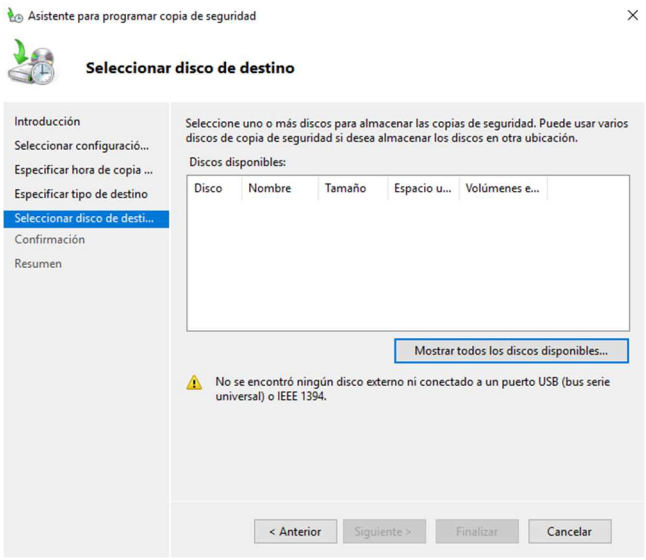
A primeira coisa que nos pergunta é quantas vezes queremos realizar a cópia por dia. Em princípio isto depende de cada empresa, da informação que é capaz de assumir que pode perder e do tempo que demore a realizar a cópia de segurança, uma vez que, como já foi indicado anteriormente, devemos realizar as cópias de segurança fora dos horários de atividade. Supondo que só quiséssemos realizar uma cópia por dia, indicaríamos a hora. De seguida, é necessário indicar onde queremos armazenar a cópia de segurança:



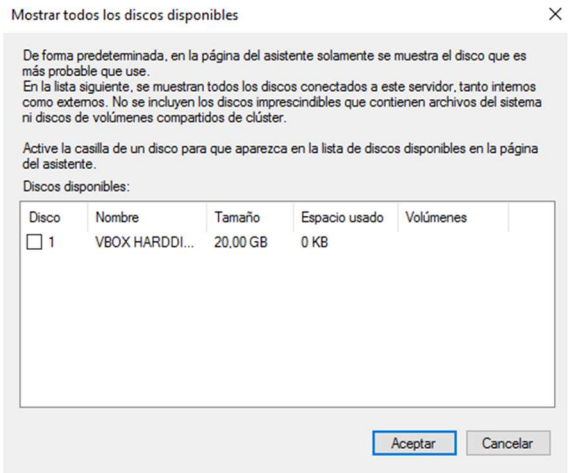
A melhor opção é a primeira, dedicando um disco exclusivamente para guardar as nossas cópias. Além disso, esse disco não deve estar no mesmo servidor, uma vez que se o eventual problema for físico, a informação e a sua cópia de segurança podem-se perder. Por outro lado, e apesar de se poderem usar discos usb, é recomendável a utilização de dispositivos NAS que ofereçam redundância a falhas, ou seja, que disponham de vários discos para que, se um falhar, a informação não se perca, porque também é distribuída entre os restantes discos. Atualmente este tipo de dispositivos têm preços acessíveis e permitem acesso e backup local e remoto.

A opção menos recomendável é usar uma unidade de rede, dado que existem Ransomwares que, além de encriptar os discos rígidos locais dos servidores, também encriptam todas as unidades de rede, pelo que ficaríamos sem informação e sem cópias de segurança.

Neste momento, selecionamos o disco no qual vamos guardar as cópias de segurança:

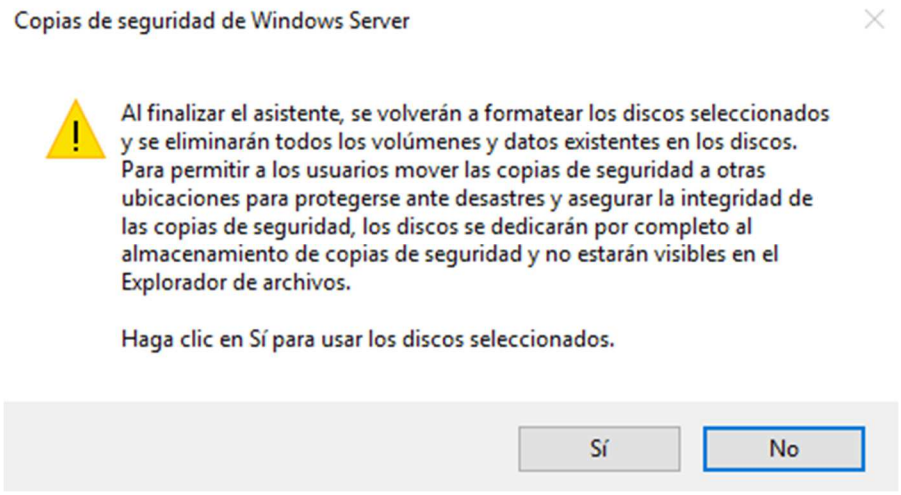


Acedemos a “Mostrar todos os discos disponíveis” e, no nosso caso, mostra-nos um disco virtual que temos criado para a demonstração, o qual selecionamos:

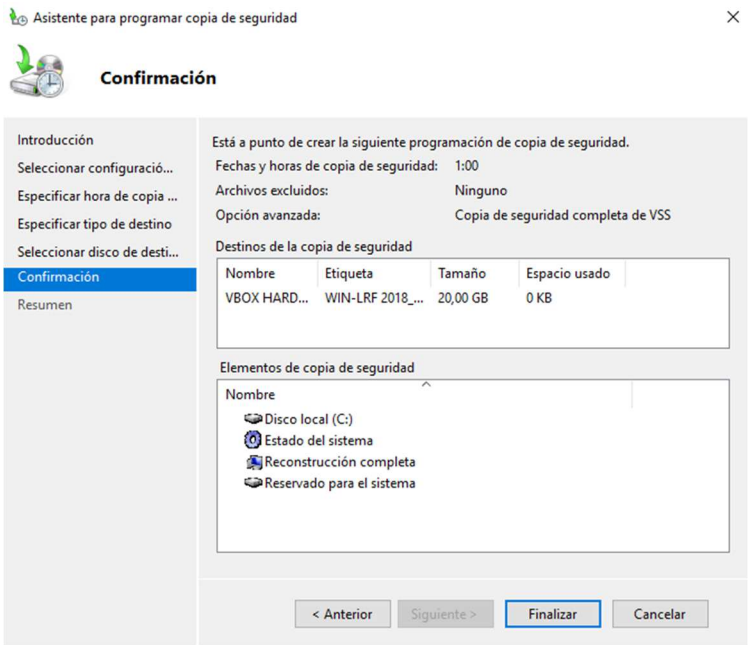


Uma vez selecionado, voltaremos à janela anterior. No caso de termos mais de um disco para armazenar cópias de segurança, apareceriam mostrados nesta lista, tendo que escolher o que nos interessa em cada ocasião.

Clicamos em "Seguinte" e continuamos. Agora, ser-nos-á indicado que este disco será usado exclusivamente para armazenar cópias e que deve ser formatado, portanto, não devemos usar discos com informação guardada porque ela será eliminada.



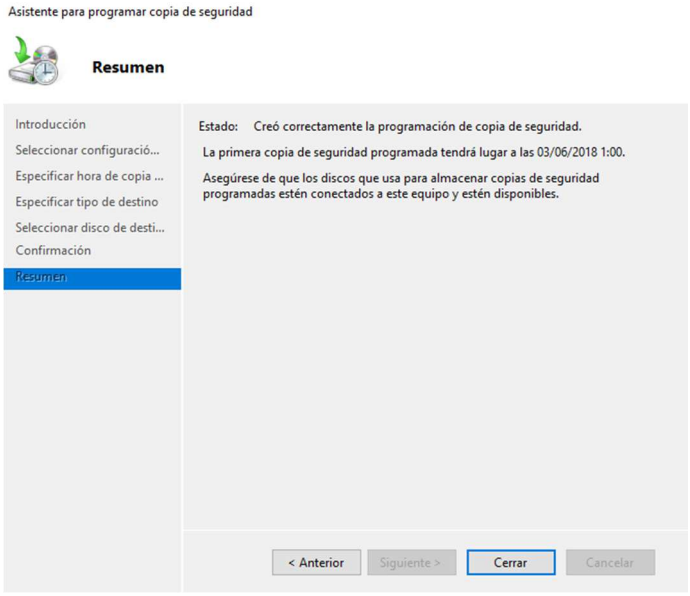
Indicamos que queremos continuar clicando em "Sim":



Neste momento, devemos verificar se a seleção das opções escolhidas está correta e, se estiver correta, clicamos em "Finalizar".

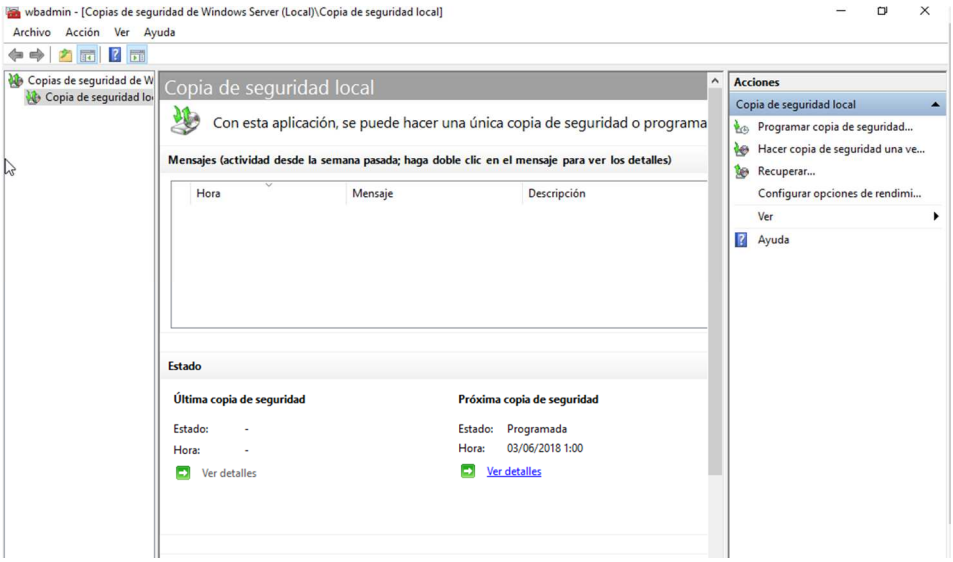
Neste processo, é formatado o disco e é gerada a programação que indicámos no processo de configuração da cópia.

Se tudo foi executado corretamente, irá surgir uma mensagem de que o processo de configuração da cópia de segurança foi realizado corretamente, conforme a seguinte imagem:

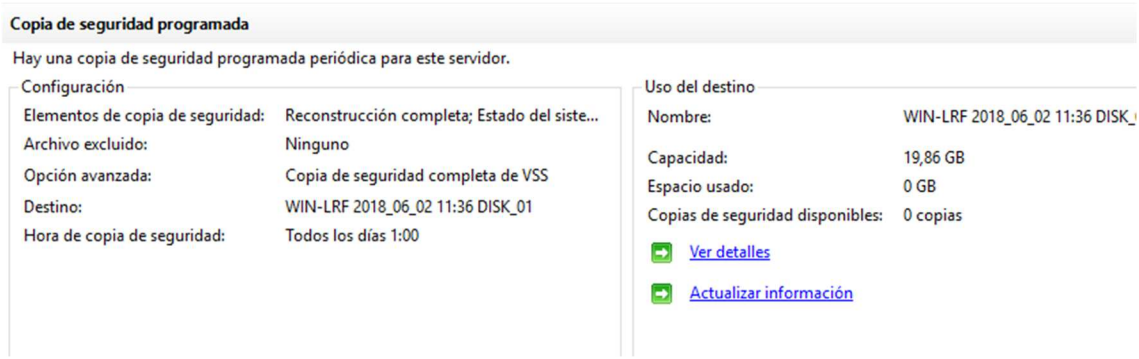


A primeira cópia não será realizada até chegar a hora definida aquando da programação do periódica do sistema.

Quando finalizarmos o assistente, aparecerá no ecrã principal a cópia que programámos:



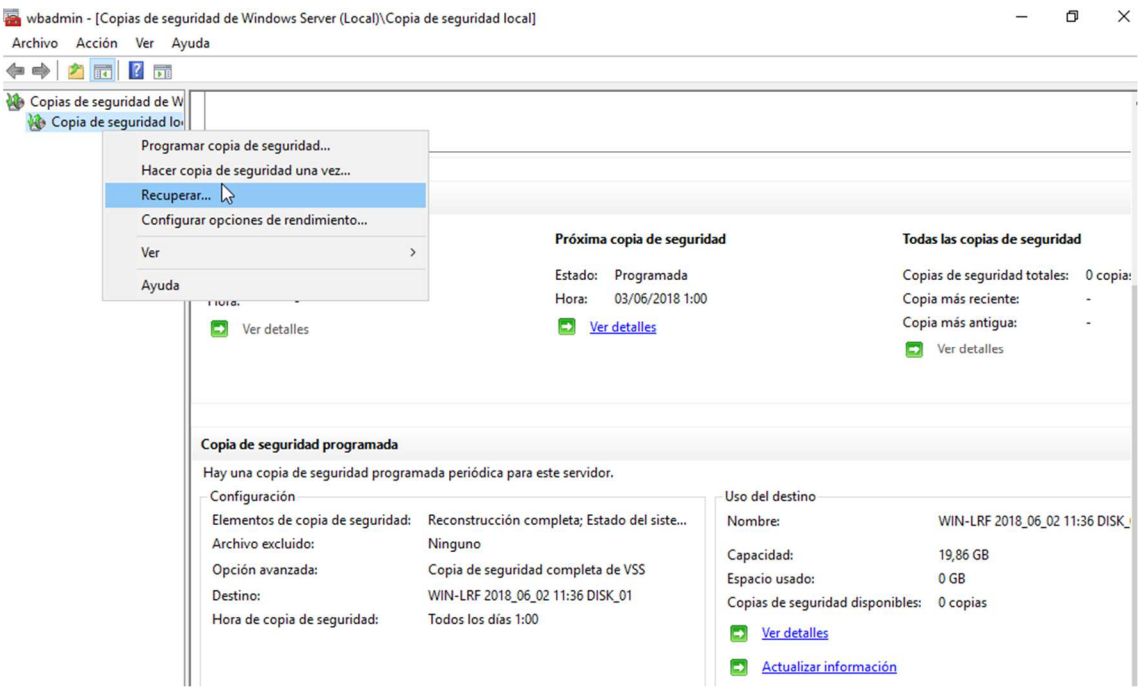
E se descermos um pouco com a barra de deslocamento vertical, veremos a informação relativa à seguinte cópia de segurança que será realizada com base na programação que realizámos:



Também indica, à direita, em que disco vai ser armazenada, qual é a capacidade total do disco, quanto espaço tem sido utilizado até agora, quantas cópias de segurança armazenou e inclusivamente permite-nos ver mais detalhes sobre as cópias.

Por outro lado, devemos verificar com frequência se as cópias de segurança estão a ser realizadas corretamente e, periodicamente, realizar um processo de restauração das cópias para ter certeza absoluta de que no dia em que tenhamos um incidente grave não teremos nenhum problema para recuperar a última cópia de segurança que temos.

Este processo pode ser feito através da opção “Recuperar”:



É um processo inverso ao anterior em que seguindo o assistente de recuperação será necessário indicar:

- Se a cópia está armazenada neste servidor ou noutra localização.
- Uma vez a localização selecionada, indicamos a data em que queremos recuperar a cópia, uma vez que estas aparecem ordenadas cronologicamente, à medida que vão sendo realizadas.
- De seguida, indicamos que tipo de recuperação queremos e que elementos queremos recuperar. No caso de ser o servidor completo, todas as opções teriam que ser selecionadas.
- Indicamos seguidamente para onde queremos recuperar a informação e confirmamos a ação depois de rever o resumo das ações que temos selecionadas.

Como foi possível ver, o processo de criação de cópias de segurança e posterior recuperação tem por base um conjunto de assistentes, bastante bem explicados, nos quais, sem grandes conhecimentos poderemos realizar ou programar a realização das nossas cópias de segurança.

Insistindo indicado anteriormente, devemos verificar frequentemente se as cópias estão a ser realizadas corretamente e que podemos recuperá-las. Desta forma evitaremos surpresas desagradáveis no dia em que, por obrigação, tenhamos que realizar um processo de recuperação da nossa informação.

4.3. SENHAS SEGURAS.

As senhas são o sistema mais usado para nos autenticarmos durante o acesso a algum tipo de serviço. No entanto, estas são uma das principais dores de cabeça dos profissionais responsáveis pela segurança das organizações.

Porquê? Sobretudo, por causa da incapacidade que temos para nos lembrarmos de mais de três ou quatro senhas complexas. Habitualmente, todos usamos as mesmas três ou quatro senhas para aceder a tudo: desde redes sociais a serviços bancários, passando pelos inícios de sessão nos nossos computadores.

O problema é que quando uma das nossas senhas é comprometida, todos os serviços onde usamos essa mesma senha ficam comprometidos.

Seguindo algumas regras simples, minimizamos enormemente o problema, no entanto, muito poucas pessoas as aplicam:

- Utilizar uma senha para cada serviço.
- Utilizar senhas complexas, que combinem números, letras (maiúsculas e minúsculas) e caracteres especiais.
- Utilizar senhas que não estejam vinculadas a dados pessoais: datas de nascimento, nomes de parentes ou animais de estimação, ...
- Alterar as senhas de forma regular.

- Utilizar dois fatores de autenticação: pins enviados para o telemóvel, cartões de coordenadas, ... Ainda que usemos este tipo de sistema no acesso à banca online, tendemos a não o fazer aquando do acesso a outros serviços ou sistemas.
- Utilizar algum serviço de gestão de senhas centralizado.

Por outro lado, o problema das senhas aumenta no espaço de trabalho visto que, ou simplesmente não as usamos, ou todos os colegas conhecem as senhas de todos, ou temos as ditas senhas apontadas em post-its colados aos monitores, ...

Se tivermos em conta que a única coisa de que um cibercriminoso precisa para aceder aos nossos sistemas é um nome de utilizador e uma senha, devemos entender o problema que surge se não gerimos corretamente as senhas da nossa empresa.

É mais do que evidente que o uso de senhas não é, nem de longe, o melhor sistema para garantir acesso seguro aos serviços que precisamos de utilizar (mais por culpa nossa do que porque o sistema não seja robusto se for utilizado devidamente). Está-se a trabalhar no sentido de encontrar sistemas que substituam a necessidade de utilizar senhas, como, por exemplo, os sistemas biométricos, o uso do smartphone, ...

Alguns destes sistemas, já disponíveis, chamam à atenção pela sua originalidade:

- **O uso do nosso coração para nos identificar:**

  O sistema utiliza um **Radar Doppler** de baixa intensidade para medir o batimento cardíaco de uma pessoa e mais tarde monitoriza-o continuamente para lhe conceder acesso ao seu computador ou a uma área restrita.

  Podem analisar mais informação no link: https://goo.gl/m9ZM1L

- **PalmSecure ID Login da Fujitsu:**

  A nova solução da Fujitsu **que lê as veias da palma da mão e seu oxigénio é** uma nova solução de autenticação biométrica que ajuda as organizações a proteger as suas redes contra o acesso não autorizado, reduzindo ao mesmo tempo o risco de ataques de cibercriminosos e phishers.

  Podem analisar mais informação no link: https://goo.gl/WysgTp

Em síntese, devemos ter presente que a boa gestão das senhas reduz a possibilidade de sofrer um incidente de segurança, explicando aos trabalhadores a importância de usar senhas seguras e os riscos que estamos assumindo quando utilizamos as senhas como a maioria vem fazendo até agora.

4.4. DISPOSITIVOS MÓVEIS.

Os dispositivos móveis, portáteis que usamos há anos, e tablets e smartphones, que usamos há pouco tempo para nos facilitar o trabalho e a nossa mobilidade, são outra das fontes de problemas desde que habitualmente não os integremos nas nossas políticas de segurança.

Graças a este dispositivo houve uma quebra no "perímetro" que os especialistas em segurança defendem. Este argumento é relevante pois há uns anos atrás proteger o perímetro da nossa infraestrutura era suficiente.

Este perímetro era definido pelos nossos routers através dos quais os nossos equipamentos comunicam com o exterior. contudo, hoje há quase mais dispositivos fora da empresa acedendo a recursos internos do que equipamentos informáticos internos. Esta situação representa um problema porque precisamos de proteger todos estes dispositivos e as comunicações necessárias para desenvolverem a sua atividade.

PORQUE PRECISAMOS DE PROTEGER ESTES DISPOSITIVOS?

Fundamentalmente porque com eles acedemos a recursos internos e neles armazenamos informação confidencial, como, por exemplo, e-mails, dados de contato de clientes e fornecedores, documentos, tais como orçamentos, projetos e fotos, credenciais de acesso (nome de utilizador | senha), ...

Além disso, em muitas ocasiões, para aceder a estes serviços ligamo-nos a redes inseguras, tanto nas nossas residências, como em hotéis, restaurantes, aeroportos, ..., sem implementar algum sistema de acesso seguro que garanta uma comunicação protegida de ponto-a-ponto e na qual a informação enviada seja encriptada.

Lembre-se que, digam o que disserem os fabricantes (tudo é publicidade), tão inseguros são os dispositivos baseados em Android, como aqueles baseados no IOS da Apple ou os da Microsoft, estes últimos numa percentagem muito pequena em comparação com os outros dois.

COMO PODEMOS PROTEGER OS NOSSOS DISPOSITIVOS?

- Usando senhas ou padrões.
- Tendo anotado o IMEI para bloquear o dispositivo em caso de roubo ou perda. Hoje, esta informação costuma estar disponível no site do provedor de comunicações, quando acedemos ao nosso espaço pessoal. Se não a localizarmos, devemos entrar em contato com a operadora por telefone.
- Utilizar dois dispositivos diferentes, um no âmbito pessoal e outro no âmbito profissional.
- Encriptar o dispositivo. Esta é uma opção de segurança que todos os dispositivos permitem hoje, mas que quase ninguém usa.
- Tendo instaladas aplicações de controlo remoto do dispositivo que nos permitam:
    - Saber onde está por georreferenciação.
    - Eliminar a informação.
- Realizando cópias de segurança da informação do dispositivo na nuvem ou nos equipamentos internos da empresa.
- Instalando software antivírus.
- Evitando fazer rooting ou jailbreaking dos dispositivos. Estes são procedimentos que permitem desbloquear os dispositivos para ser possível instalar aplicações não oficiais ou instalar apps oficiais sem ter de pagar por isso.

- Assegurando-nos de que as apps que utilizamos são legítimas, mesmo se as transferirmos das lojas oficiais da Google, Apple ou Microsoft.
- Não utilizando apps gratuitas. Quando algo é grátis, o preço somos nós mesmos (a nossa informação).
- Atualizar os sistemas operativos dos dispositivos quando os fabricantes oferecerem atualizações que, além de nos trazerem novas funcionalidades, corrigem vulnerabilidades detetadas.

COMO PODEMOS PROTEGER NOSSAS COMUNICAÇÕES?

- Tentando evitar redes públicas.
- Utilizando ferramentas de VPNs, Redes Privadas Virtuais, que autenticam a conexão desde o exterior (utilizador | senha e encriptam a informação que é transmitida).
- Utilizando sistemas de escritório remoto, como Citrix, Parallels, VmWare ou outros, que permitem o acesso a informação e recursos da organização, desde o exterior, evitando a necessidade de ter essa informação armazenada no dispositivo.
- Incorporar os dispositivos móveis nas políticas de segurança dos sistemas de servidores e geri-los do mesmo modo que gerimos os equipamentos internos, com Políticas de Grupos no Windows Server (GPOs), por exemplo.

CONCLUSÕES

Temos uma arma muito poderosa nas nossas mãos, o que nos permite ser muito mais produtivos se a usarmos como devemos, mas que quando utilizada de forma inadequada, perdida ou infetada com malware (que permita monitorizar as nossas comunicações ou aceder ao interior dos nossos sistemas quando ligamos o nosso dispositivo aos nossos equipamentos informáticos), pode causar graves prejuízos à empresa.

Entenda que estes dispositivos são como qualquer outro equipamento da sua organização que você deve proteger e integrar nas políticas de segurança. É preciso tê-los muito mais vigiados porque, ao contrário dos restantes dispositivos, estes saem da sua empresa levando informação confidencial que não deve cair nas mãos de terceiros.

Use os seus dispositivos com bom senso. Na maioria dos casos, isso já minimiza o risco do nosso dispositivo móvel causar um incidente de segurança na nossa empresa.

Finalmente, devemos desenvolver periodicamente formações / consciencializações com os nossos trabalhadores para que estes compreendam o risco que assumem ao utilizar os referidos dispositivos e como podem ser evitados os riscos causados pelo uso inadequado.

Se vamos permitir que os nossos trabalhadores utilizem os seus dispositivos pessoais (portáteis, tablets, smartphones ou pens / discos usbs), o que hoje é chamado BYOD (Bring Your Own Device) implemente as medidas de segurança adequadas.

Assuma que quando tentam atacar a sua empresa este ataque é sempre feiro através do elo mais fraco e este é sempre o trabalhador. Vamos comprometer o trabalhador, infetar os seus dispositivos e aceder aos sistemas internos da empresa através deles.

4.5. PROBLEMAS DE SEGURANÇA NAS NOSSAS REDES. REDES WIFI.

Neste ponto, vamos fazer referência à segurança das redes wi-fi que gerimos. As considerações sobre como usar os nossos dispositivos móveis com segurança em redes wi-fi públicas, que não controlamos nem gerimos, já foram acima indicadas.

Nas nossas empresas, podemos ter uma das seguintes situações:

1. O router de acesso à Internet é, simultaneamente, o nosso ponto de acesso wi-fi.
2. Utilizamos um router para aceder à internet e temos APs (pontos de acesso) wi-fi aos quais nos conectamos com os nossos dispositivos móveis.

No primeiro caso, devemos ter um cuidado especial, porque comprometer o router pode causar muitos mais problemas de segurança do que se apenas comprometermos os APs wi-fi.

No entanto, na maioria dos casos, comprometer o router é muito simples, já que praticamente ninguém altera as credenciais de acesso ao dispositivo.

Quando contratamos o serviço de telefone e internet com uma operadora de comunicações, um técnico da mesma vem fazer a instalação do router que nos fornece o serviço. Este verifica que o serviço está operativo, fornece-nos a chave para aceder ao wi-fi e sai. O que este técnico não nos diz é que todos os routers têm um utilizador "administrador" com uma senha inicial (igual para todos os dispositivos da mesma marca/modelo) que usaremos quando quisermos aceder ao dispositivo para o configurar: serviço DHCP, DNS, Firewall ou alterar o SSID e a senha por defeito do wi-fi, entre outros aspetos.

Sabendo qual é a marca e o modelo do router e fazendo uma busca no Google, leva 30 segundos a saber qual é o nome do utilizador administrador e sua senha inicial para aceder o dispositivo.

O melhor de tudo é que não precisamos de estar perto. Podemos aceder aos dispositivos através de uma ligação remota, através do endereço IP público do router e isso pode ser obtido usando software analisador de redes como o Shodan ou outros.

Uma vez que conhecermos o IP público, o utilizador e a senha da conta do administrador poderemos aceder ao dispositivo e alterar a configuração para:

- Modificar os endereços IP dos servidores DNS para que todas as consultas de resolução de nomes passem pelos nossos DNS. Isto permitirá a quem está a aceder indevidamente à rede, saber a quais serviços os trabalhadores estão conectados.
- Captar e analisar o tráfego de saída do router para tentar obter utilizadores e senhas de serviços internos.

Modificar as tabelas ARP do router. Este é um procedimento pelo qual os endereços IP se vinculam aos endereços MAC dos dispositivos. Desta forma conseguimos que apenas os nossos dispositivos acedam à nossa rede e, portanto, aos nossos serviços.

- Alterar o SSID das nossas redes wi-fi ou alterar os códigos de acesso a estas redes, causando um ataque de negação de serviço (DoS), impedindo que os utilizadores possam aceder à rede wi-fi.

SEGURANÇA NAS NOSSAS REDES WI-FI

Este sistema simples de instalar, configurar e gerir representa uma economia de custo importante, evitando ter que instalar redes cabladas para que os nossos utilizadores se conectem aos serviços e recursos necessários para desenvolver sua atividade, acedendo assim através de ligações sem-fios.

O problema é que não podemos limitar o sinal wi-fi impedindo que alguém de fora da nossa empresa se possa conectar.

Por esta razão, devemos:

- Alterar periodicamente a senha de acesso ao wi-fi e verificar que a senha é suficientemente robusta para resistir a um ataque pela força bruta.
- Não partilhar a chave do wi-fi com ninguém.
- Se precisarmos que pessoas externas à empresa acedam ao nosso wi-fi, configure um SSID específico para isso. Neste novo SSID:
    - Vamos limitar a largura de banda que permitimos usar.
    - Não se poderá ligar a recursos e serviços internos.
    - Vamos filtrar o tipo de páginas que podem ser visitadas, evitando o acesso a páginas com conteúdos inadequados através das quais podem ser transferidos conteúdos protegidos por propriedade intelectual, ...

Deve ter em conta que somos, em parte, responsáveis se um utilizador realizar qualquer ato criminoso utilizando para isso a nossa infraestrutura informática. Como veremos a seguir, com o novo Regulamento Geral sobre Proteção de Dados, que substitui a antiga Lei Orgânica de Proteção de Dados, a segurança deve ser proativa e já não vai servir o "não sabia".

5. LEGISLAÇÃO E REGULAMENTAÇÃO DE SEGURANÇA. NOVO RGPD.

Os cibercrimes crescem exponencialmente como a própria tecnologia. A Europol já indicou, no final de 2016, que há já países em que, em termos percentuais, os cibercrimes ultrapassam os crimes tradicionais.

O problema com essa situação é que a legislação, muito mais lenta que a tecnologia, fica sempre atrás destes novos cibercrimes. Estamos a ser hoje em dia vítimas de crimes que não existiam há 5 anos e em 5 anos seremos afetados por crimes que não existem hoje.

Perante esta situação só nos resta cumprir a legislação e regulamentos em vigor em cada momento, dado que em algumas ocasiões os nossos sistemas são comprometidos para cometer tais crimes.

Cumprir com a lei permitir-nos-á respeitar os direitos daqueles que estão vinculados à nossa atividade: clientes, fornecedores, trabalhadores, ..., e permitir-nos-á evitar sanções que, como veremos, com o novo RGPD, que desde 25 de maio deste ano nos afeta, podem chegar aos 20 milhões de €, ou a 4% da nossa faturação, em casos muito graves.

Até 25 de maio de 2018, em Espanha, havia as seguintes leis vinculadas à segurança da informação:

- Lei Orgânica 15/99 sobre Proteção de Dados, também conhecida como LOPD.
- Lei 34/2002 sobre Serviços da Sociedade da Informação e Comércio Eletrónico (LSSI).
- Lei 32/2003 Geral de Telecomunicações.
- Lei 59/2003 de Assinatura Eletrónica.
- Real Decreto Legislativo 1/1996 sobre Propriedade Intelectual.
- Lei 17/2001 sobre Propriedade Industrial.
- Lei 11/2007 sobre Acesso Eletrónico a Serviços Públicos.
- Alguns setores têm a sua própria legislação, como, por exemplo, o agrário.
- Outros, como a Banca, dispõem de regulamentação internacional.

Estas leis procuravam proteger pessoas físicas e jurídicas daqueles crimes que são cometidos contra eles:

- Contra sua privacidade, através da venda de dados. Lembre-se de que não há nada de graça e quando aceder a serviços gratuitos está a pagar com a sua privacidade e com a informação que está a gerir através da interação com a internet.
- Referidos à distribuição de conteúdos ilegais através da rede, como por exemplo, os referidos à distribuição de pornografia infantil.
- Crimes económicos: roubo, extorsão, usurpação de identidades bancárias, ...
- Crimes contra a propriedade intelectual. Em Espanha, ainda "pirateamos" mais de 50% do software que utilizamos nas nossas empresas e residências.

Algo que podemos observar à primeira vista, quando olhamos para as leis e crimes que descrevemos anteriormente, é que:

- As leis são antigas. Entre 10 e 20 anos, no mundo da tecnologia, é demasiado tempo. Se se lembra de como era, tecnologicamente, a sua empresa há 15 anos, perceberá que não tem nada a ver com a realidade atual.

Os crimes atuais (cibercrimes), mantendo os descritos, aumentaram em número e tipo. Os cibercrimes são divididos em dois tipos:

- Aqueles que se aproveitam da tecnologia como meio para ocorrer:
  - Contra a honra, como os crimes de ódio através de redes sociais.
  - Cyberbullying.
  - Ameaças e coações.
  - Crimes sexuais, como pornografia infantil.
- Aqueles que atacam as nossas infraestruturas:
  - Acesso e intercetação ilícita.
  - Interferência em dados e sistemas.
  - Falsificação informática.
  - Fraude informática.
  - Contra a proteção industrial intelectual.
  - Contra a saúde pública.

Se quiser obter mais informação, visite o site do Observatório Espanhol de Crimes Cibernéticos (http://oedi.es):

- Na secção de cibercrimes, é possível aprender mais sobre cada um dos tipos acima enunciados.
- Na secção de estatísticas, é possível observar o crescimento, ano a ano, deste tipo de crimes.

Outro problema que existe, e que vai crescendo, ligado aos cibercrimes é que:

- Não há um número suficiente de peritos judiciais informáticos. Estes são os encarregados de recolher as evidências tecnológicas do crime cometido. São como o CSI dos crimes tradicionais. O trabalho do perito é fundamental para que as evidências obtidas possam ser tidas em consideração pelo Juiz que julgue o caso.
- Em segundo lugar, há muito poucos ciberadvogados, com formação legal e tecnológica, preparados para entender o crime tecnológico acontecido, de modo que estes crimes continuam a ser tratados como crimes tradicionais.
- Em terceiro lugar, não temos um número suficiente de juízes, com formação tecnológica que sejam capazes de entender as provas que lhes são apresentadas.
- Não há formação específica sobre estas disciplinas.

Há 25 anos que existe um novo continente, por outro lado, o mais populoso de todos, chamado ciberespaço. Usamos este ciberespaço todos os dias na nossa vida pessoal e profissional e o seu uso suscita certos problemas dos quais muitas vezes não estamos cientes:

- Não tem fronteiras físicas, além de que as máquinas desde as quais os ataques cibernéticos são realizados estão num país físico, no qual é muito provável que as disposições legais

sejam muito menos restritivas. Por isso, não é afetado pela territorialidade, base da jurisprudência atual.
- A tecnologia permite que, na maioria dos casos, não consigamos saber onde os ataques são produzidos, nem possamos identificar os autores.
- Não está legislado e não há poderes legislativo nem judicial.

Este ciberespaço é já considerado há anos como o quinto ambiente estratégico, atrás da terra, do ar, do mar e do espaço, ainda que, ao contrário destes, o ciberespaço não possui nenhum tipo de regulação normativa.

O NOVO RGPD

A seguinte legislação, que nos afetava até 25 de maio, foi revogada:

- A LOPD 15/1999.
- O Real Decreto 1720/2007.
- A Instrução 1/2006 de Sistemas de Videovigilância.
- A Diretiva 95/46 do Parlamento Europeu.

No seu lugar, estamos atualmente obrigados por:

- O novo Regulamento Geral de Proteção de Dados Europeu.
- No futuro próximo, a nova Lei Orgânica de Proteção de Dados, da qual apenas o anteprojeto é conhecido.

O novo Regulamento visa unificar critérios, a nível europeu, em todas as questões relacionadas com o tratamento de dados pessoais e, portanto, afetará todas as empresas, independentemente do seu tamanho e atividade, que desenvolvem a sua atividade em qualquer um dos países europeus, ou qualquer empresa cuja sede social esteja localizada fora do âmbito europeu, mas que prestem serviços aos utilizadores europeus.

Os princípios relativos ao tratamento da informação que tratamos baseiam-se em:

- A minimização dos dados que recolhemos. Ou seja, recolheremos apenas aqueles dados que são imprescindíveis.
- Estes dados devem ser exatos e devem estar atualizados.
- Devemos estabelecer o limite da finalidade para a qual os dados foram recolhidos.
- Temos de cumprir os princípios de legalidade, lealdade e transparência.
- Devemos limitar o prazo de conservação dos dados de acordo com a duração da prestação de serviços e as obrigações legais que nos afetem.

Os dados podem ser obtidos:

- Do próprio interessado: devemos informá-lo no mesmo momento em que obtemos os dados.
- Ou de um terceiro, tendo que informar no prazo de um mês a partir da data de obtenção dos dados e sempre no primeiro contato que estabelecermos.

O tratamento dos dados deve basear-se em:

- Uma relação contratual.
- Uma obrigação legal para o responsável pelo tratamento.
- Um interesse:
    - Vital para o interessado.
    - Público ou exercício de poderes públicos.
    - Legítimo que prevalece do responsável ou terceiros a quem os dados sejam comunicados.
- Consentimentos.

Quanto ao consentimento, este deve ser inequívoco. Não são admitidos consentimentos tácitos ou por omissão, nem são admitidos checks pré-selecionados, devendo ser o mais explícito possível.

Como acontecia com a LOPD, o Regulamento considera uma série de Direitos que defendem os interesses do titular dos dados:

- Direitos ARCO: Acesso, Retificação, Cancelamento (agora Supressão) e Oposição.
- Além disso, são incorporados os seguintes direitos:
    - Esquecimento.
    - Limitação do tratamento.
    - Portabilidade.

Relativamente ao Encarregado do Tratamento, o Regulamento obriga a contratar encarregados para garantir o cumprimento do RGPD. Esta garantia pode ser acreditada:

- Através de formação certificada.
- Através da certificação de anos de experiência no tratamento de dados pessoais. Por exemplo, os profissionais que geriram a LOPD nos últimos anos.

O RGPD obriga-nos a mudar de paradigma. Até agora temos tido uma mentalidade reativa relativa à segurança, no entanto, o Regulamento exige que a nossa segurança seja proativa, condicionando as medidas de segurança ao risco que cada um assume no tratamento de dados de terceiros.

Para alcançar isto, seremos obrigados a realizar uma análise exaustiva dos riscos que nos podem afetar, classificando e quantificando a probabilidade de um risco se materializar e o impacto que provocaria.

Além de analisar o risco, devemos avaliar o seu impacto. Tenha em conta que

RISCO = PROBABILIDADE X IMPACTO.

Uma das obrigações que mais chama a atenção é o facto de ter que informar a Comissão Nacional de Proteção de Dados, quando tivermos sofrido um incidente de segurança, no qual dados pessoais tiverem sido afetados, no prazo de 72 horas desde que foi detetado esse incidente.

Teremos que informar sobre:

- A natureza e categoria do incidente.
- O número de afetados.
- Quem é o Encarregado de Proteção de Dados, se tivermos.
- As consequências causadas.
- Nos casos em que a gravidade do incidente represente um alto risco para os direitos e liberdades dos titulares dos dados, devemos informar os interessados.

O Encarregado de Proteção de Dados (EPD) é uma nova figura que aparece com o novo Regulamento. Nem todas as empresas têm a obrigação de ter um. Sim têm a obrigação:

- Organismos Públicos.
- Empresas que tratam dados em larga escala.
- Colégios Oficiais.
- Empresas do setor de saúde.
- Centros educativos.
- Entidades seguradoras.
- Empresas de publicidade e prospeção comercial.

Não é obrigatório para empresas com menos de 250 trabalhadores, desde que não tratem informação que possa afetar os direitos e liberdades dos titulares.

Poderá ser EPD qualquer pessoa com conhecimentos de legislação e experiência no tratamento de dados pessoais ou aquelas pessoas que superarem a formação certificada para esse efeito.

Como novidade importante, deixou de ser obrigatório registar os ficheiros, conforme exigido pela LOPD.

Agora precisaremos ter um registo das atividades que deve conter:

- Nome e informações de contacto do Encarregado.
- Finalidades do tratamento.
- Descrição das categorias dos interessados e categorias dos dados tratados.

Há novidades quanto a:

- Os sistemas de videovigilância.
- O tratamento de dados de menores, sendo necessário o consentimento dos tutores legais dos menores de 13 anos.
- O tratamento de dados de falecidos, podendo os seus herdeiros solicitar o acesso aos dados, sua retificação ou até mesmo sua supressão.

Por último, mas não menos importante, as razões pelas quais devemos cumprir o RGPD:

- Não podemos exigir que alguém trate os nossos dados de acordo com a lei, se nos não o fizermos.
- Para evitar sanções, que aumentaram de uma forma muito importante:
    - Sanções graves: até 10 milhões de € ou 2% da faturação.
    - Sanções muito graves: até 20 milhões de € ou 4% de faturação.

Imagine o que teria custado ao Facebook a recente sanção imposta pela AEPD, pelo uso indevido de dados pelo WhatsApp, tendo em conta que foi sancionado com 600.000€, a mais alta sanção aplicada à luz da anterior LOPD.

Temos de dar um tempo ao novo RGPD para ver como se incorpora no dia-a-dia das empresas, no entanto, existem relatórios que afirmam que 65% das empresas em Espanha não estão preparadas para tratar a sua informação pessoal de acordo com o regulamento. E isso considerando que tivemos dois anos para nos adaptarmos.

A Agência Espanhola de Proteção de Dados informou já, semanas antes de 25 de maio, que não haverá nenhum tipo de moratória e que iniciaria imediatamente planos de inspeção para empresas de setores críticos: saúde, instituições financeiras e empresas de telecomunicações.

Se a sua empresa ainda não cumpre com o novo RGPD, não o deixe mais. Trabalhará melhor e evitará sanções.

6. PLANO DE SEGURANÇA: PREVENÇÃO, AUDITORIA E PROTEÇÃO.

Todas as empresas deveriam ter um Plano de Segurança, mas poucas o têm. Nele devem ser identificadas as ameaças que nos podem afetar, os riscos que assumimos e o impacto que provocaria na nossa atividade se um destes riscos se materializar.

Além disso, deverão ser identificadas as medidas preventivas que implementaremos, as auditorias internas ou externas que serão desenvolvidas regularmente e como nos vamos proteger quando sofrermos um incidente de segurança, definindo o denominado Plano de Resposta a Incidentes.

Existem apenas dois tipos de empresas: as que foram atacadas e o sabem e as que foram atacadas e não o sabem.

Perante esta afirmação apenas nos resta assumir que a qualquer momento podemos sofrer um incidente que possa pôr em perigo a continuidade da nossa atividade e devemos estar preparados para recuperar essa atividade no menor tempo possível e com o menor impacto possível.

As causas destes incidentes, como fomos enunciando ao longo deste manual, podem ser:

- Diretas, pelo qual poderíamos prevê-las e mitigá-las:
    - Danos materiais:
        - Inundações.
        - Incêndios.
        - Falhas elétricas
    - Erros humanos, numa percentagem muito alta de ocasiões.
    - Roubo /fugas de informações.
    -
- Alheias, por isso devemos estar atentos e à espera de que aconteçam no momento mais inesperado:

- Infeções por malware.
- Ataques dirigidos.
- Causados por os nossos fornecedores e / ou colaboradores.

Os planos de resposta a incidentes, também denominados planos de continuidade de negócio, permitem-nos ter previstas as ações que serão realizadas quando ocorrer um incidente que tenhamos catalogado, e devem ter em conta dois aspetos importantes:

- O tempo que demoraríamos a recuperar o sistema.
- O tempo máximo que poderíamos suportar com o serviço, parcial ou totalmente parado.

Estes dois fatores condicionarão, em grande parte, as medidas que teremos que implementar. Não serão as mesmas para uma empresa que se pode dar ao luxo de estar um dia inteiro sem sistemas informáticos, do que para as empresas que não podem parar mais de duas horas.

Por outro lado, não pense que isto são considerações que devem ser tidas em conta apenas em grandes empresas. Como mencionámos quando nos referimos à mudança de mentalidade que exige o novo RGPD, tendo que ser proativos e não reativos quando falamos de segurança, deveremos entender que este tipo de ações vai permitir sermos mais eficientes e mais resilientes, tendo assim um impacto positivo para a empresa face aos clientes e fornecedores.

A criação destes planos deve ser feita de acordo com a nossa realidade, ou seja, as medidas a adotar devem ser proporcionais às nossas necessidades e ter por base a definição de objetivos e processos da empresa.

Os objetivos, geralmente, centram-se na recuperação do sistema, num período mínimo de tempo, mantendo o nível de serviço dentro dos limites que tenhamos estabelecido como aceitáveis.

Os processos seguirão as fases seguintes, sempre tendo em conta a ideia de melhoria contínua, ou seja, quando chegarmos à fase final, voltaremos à primeira para melhorar continuamente o nosso plano.

Tenha em conta que as empresas e as suas infraestruturas são dinâmicas e isto influencia os nossos planos de segurança, dado que seis meses ou um ano depois de ter definido objetivos e processos, é possível que, pela prestação de um novo serviço ou a incorporação de uma nova tecnologia na nossa infraestrutura, o plano anterior não se ajuste à realidade do momento, deixando inúteis os objetivos e processos estabelecidos.

As fases que definem o nosso plano devem ser ajustadas às seguintes:

- Na fase de Análise, avaliamos ameaças, riscos e impactos a curto e médio prazo.
- Na fase de Desenho, definiremos as medidas que vamos aplicar e os procedimentos de resposta.
- Na fase de Implementação, geriremos a incorporação das medidas selecionadas e estabeleceremos um calendário de programas de formação/consciencialização para os nossos trabalhadores. Sendo o trabalhador interno o elo mais fraco da segurança, é muito

importante que entendam os riscos e as consequências de usar de maneira inadequada a tecnologia que lhes é fornecida para desenvolver a sua atividade.

- Na fase de Verificação, devemos assegurar de que o que temos desenhado na teoria funcionará corretamente no dia em que sofrermos um incidente. Às vezes, voltaremos às fases de desenho ou implementação se observarmos nesta última fase que as medidas desenhadas não são tão eficazes como pensávamos.

Quando chegarmos à fase final, voltaremos à fase de desenho para recomeçar, mesmo que os nossos processos produtivos, serviços e tecnologia não tenham mudado. De vez em quando surgem novas vulnerabilidades que nos afetam e devemos estar atentos aos novos riscos que nos espreitem.

Tudo isto pode ser apoiado com a realização de auditorias internas e, eventualmente, externas. De vez em quando é interessante que um consultor externo nos proporcione uma visão diferente da nossa, muitas vezes condicionada. Isto de quatro olhos vêem mais que dois, também se aplica nestas situações.

Estas auditorias devem ser combinadas com a execução de simulacros que nos permitam estar preparados para o dia em que tivermos de realizar todos estes procedimentos que estamos a desenvolver.

Por outro lado, é importante definir claramente quais os ativos que queremos auditar, se serão todos ou apenas uma parte.

Em definitivo, o nosso Plano de Segurança deve abordar todas as seguintes medidas, sem exceção:

- Medidas aplicadas a desastres naturais.
- Medidas aplicadas a problemas estruturais das nossas instalações.
- Medidas aplicadas a problemas de Hardware.
- Medidas aplicadas a problemas dos Sistemas Operativos: clientes / servidores.
- Medidas aplicadas a problemas de Software.
- Medidas aplicadas a problemas da rede interna e comunicações externas.
- Medidas aplicadas a problemas de cópias de segurança.
- Medidas aplicadas a problemas com a informação (CIA).
- Medidas aplicadas a problemas com pessoal interno e colaboradores externos.
- Medidas aplicadas a problemas com o património.
- Medidas aplicadas ao cumprimento normativo e legal vigente.
- Medidas aplicadas a problemas causados por outros riscos.

Como pode ver, procuramos minimizar as possibilidades de sofrer um incidente e definir como reagir quando sofremos, e ainda que possa ser um pouco simplista, podemos dizer que uma boa segurança é baseada em três aspetos fundamentais:

- O utilizador deve ter privilégios mínimos de acesso. Ou seja, só pode aceder àqueles recursos diretamente relacionados com a atividade que desenvolve.

- Exposição mínima, ou seja, só ter ativos aqueles serviços informáticos que realmente são oferecidos interna e/ou externamente.
- Termos um sistema de cópias de segurança, atualizado, que combine o armazenamento local dessas cópias com um sistema de backup em cloud, redundante, que nos permita ter a informação fora da empresa.
  Embora sejam situações um pouco extremas, pense no que aconteceu nos ataques de 11 de setembro nos Estados Unidos ou no incêndio do Edifício Windsor em Madrid.
  As empresas que não tinham cópias de segurança fora dos escritórios que estavam naqueles edifícios não puderam continuar a desenvolver a sua atividade, devido à impossibilidade de recuperar o seu ativo mais valioso.

Se controlarmos estes três aspetos, reduziremos enormemente a possibilidade de sofrer um incidente e, se o sofrermos, o tempo de reação e retorno à normalidade. O resto dos fatores a ter em conta, descritos acima, não menos importantes, devem estar alinhados com estes três fatores.

Em suma: não negligencie a segurança informática da sua empresa. Evitará perdas económicas, perdas de reputação e dores de cabeça.

CAPÍTULO 2. SEGURANÇA CLOUD PARA PMES E TRABALHADORES INDEPENDENTES.

1. SERVIÇOS DISPONÍVEIS NA NUVEM.

Quando dizemos que utilizamos serviços na nuvem, ou cloud, o que estamos a dizer é que estamos a utilizar serviços *on demand*, numa infraestrutura que geralmente não é nossa, e que normalmente se encontra na Internet.

Todos utilizamos serviços cloud já há algum tempo, quando usamos os serviços gratuitos ou pagos, do Google ou da Microsoft, entre outros provedores. Por exemplo: serviços tais como correio eletrónico, armazenamento da informação nas drives de ambos os fornecedores, ferramentas como Skype ou Hangouts, para realizar videochamadas, aplicações de escritório como processadores de texto, folhas de cálculo ou aplicações para gerar apresentações atraentes e muitas mais, algumas praticamente desconhecidas para o público em geral.

A nuvem está a começar a revolucionar os espaços de trabalho e em 15 anos, mais ou menos, terá mudado completamente as nossas empresas e escritórios.

Lembra-se de como era o seu escritório há 15 ou 20 anos? O QUE MUDOU?

Bem, nos próximos 15 ou 20 vai mudar ainda mais, basicamente porque será retirada das nossas empresas a infraestrutura que agora mantém operativos os nossos negócios.
Pense em escritórios nos quais os servidores, o armazenamento, o backup, os sistemas de segurança, as aplicações, etc., já não estão fisicamente no mesmo lugar em que estão agora, deixando apenas terminais, praticamente ”burros”, que se ligarão a estes serviços on-line, e alguns equipamentos de impressão para imprimir alguns documentos que serão impressos em papel. Hoje, existe já um número significativo de empresas que praticamente não imprime nada, usando estes dispositivos para digitalizar documentos.

Por que vai acontecer esta mudança, que já se começou a materializar?
Principalmente porque vai custar menos pagar pelo uso, em regime de aluguer, do que adquirir os equipamentos e mantê-los.
Como acontece ao comprar um carro, existem algumas despesas importantes, nas quais geralmente não reparamos.

É claro que nem todas as empresas têm as mesmas necessidades, mas alguma vez parou para pensar no custo da infraestrutura tecnológica da sua empresa?

- As salas que devemos estar preparadas para albergar a nossa infraestrutura mais crítica, com tetos e pisos técnicos.

- Devem existir sistemas de refrigeração e sistemas anti-incêndios.
- Devem existir sistemas de identificação de acesso.
- Devem existir armários e cabines.
- Os próprios servidores: controladores de domínio, servidores de base de dados, de armazenamento, de backup, ...
- Todo o equipamento de comunicações e segurança: Routers, Firewalls, IDS / IPS, ...
- O Suporte técnico de todos estes equipamentos.
- A energia necessária para manter tudo isto disponível para acesso 24 horas por dia.
- Pessoal que o mantenha operacional e seguro. E, além disso, cumprindo com todas as normativas e leis vigentes evitando assim possíveis sanções.

Ainda pensa que é mais barato comprar do que pagar pelo uso? Bem, neste momento já não o é, mas em poucos anos, quando o mercado para este tipo de serviços estiver mais estável, será muito mais barato ir para a nuvem do que ficar em terra.

Se o aspeto económico nos agrada, temos de assumir que a reparação da nossa própria informação não está no nosso poder, sendo a solução o seu armazenamento em máquinas de um provedor de serviços no qual temos de confiar.

E a questão é: realmente acredita que as suas informações e serviços estarão mais seguros nas suas instalações do que se as tiver nos centros de dados de empresas como a Amazon, a Google, a Microsoft, a IBM, ...? É evidente que as instalações destes operadores, os sistemas de redundância, ..., serão inatingíveis para PMEs. Estas empresas possuem dezenas de CPDs, localizados em todo o mundo, a replicarem a nossa informação para que, em caso de desastre em qualquer um deles, a informação seja distribuída pelos restantes e o nosso serviço não seja afetado pela falta de disponibilidade da mesma.

Mesmo prestando atenção às inúmeras vantagens fornecidas por este sistema, devemos reconhecer que este serviço pode não encaixar para um pequeno tipo de empresas devido à sua idiossincrasia.

Por esta razão, devemos realizar um estudo prévio para identificar se o nosso negócio pode beneficiar da adoção deste tipo de serviço e, se for o caso, devemos dimensionar de forma correta a nossa necessidade. E isto não é trivial.

Por outro lado, a flexibilidade e a escalabilidade, destes serviços, e a possibilidade de aceder aos seus recursos desde qualquer lugar, num momento em que a mobilidade se tornou essencial para a gestão dos nossos negócios, são mais uns motivos para decidir dar o salto para a nuvem.

Mas, a que nos estamos a referir quando falamos de flexibilidade e escalabilidade?

Fundamentalmente à capacidade de dimensionar a minha infraestrutura de acordo com as minhas necessidades em cada momento, de uma forma quase imediata.

Suponha que adquire um servidor para um novo serviço que precisa fornecer aos seus trabalhadores. 6 meses depois, você precisa de aumentar o pessoal num número de trabalhadores

com o qual não tinha contado quando dimensionou o servidor que comprou e precisamos de o expandir porque ficámos inicialmente aquém das reais necessidades de escala.

Numa situação tradicional, teríamos de entrar em contato com um ou vários fornecedores, solicitar um orçamento, realizar uma encomenda, esperar vários dias pela chegada do material comprado proceder à sua instalação. Isto, em máquinas de gama média, significa parar o servidor, instalar o novo hardware, reconfigurá-lo e reiniciar a máquina.

Ao lermos a explicação dada acima podemos perceber da complexidade da operação. Num serviço de cloud apenas teríamos realizado uma extensão dos recursos das nossas máquinas na nuvem, pagando a partir desse momento pelo serviço recebido.

Continuando o exemplo anterior, imagine agora que algum tempo depois, o pessoal incorporado deixa de ser necessário, porque tinha sido contratado para um projeto específico. Nesse momento, não podemos simplesmente contactar o vendedor que nos forneceu o equipamento para efetuar uma devolução porque já não precisamos dele. No entanto, no tempo que demorámos a ler esta nova explicação, num ambiente cloud teríamos redimensionado novamente os nossos equipamentos, para baixo (downgrade), pagando a partir daquele momento pela nova configuração que passaríamos a usar.

Outra situação, que infelizmente acontece com frequência, é quando compramos um equipamento que pagamos por meio de crédito, um renting ou um leasing, e se dá a circunstância de termos que encerrar a nossa atividade. Neste caso, temos que terminar de pagar o equipamento adquirido sem poder recuperar o investido porque o valor do produto tem vindo a desvalorizar de tal forma que este já nem sequer vale o que se deve. No entanto, se utilizarmos serviços em nuvem e houver uma situação como a descrita, basta informar o provedor de serviço que aquele mês será o último que iremos subscrever o serviço e o problema termina.

Um dos principais obstáculos que podemos encontrar ao implementar estas soluções é a necessidade de ter uma conectividade à Internet muito boa para poder aceder aos serviços. Se não existe conexão à Internet, não há serviço.

É verdade que em áreas urbanas isto não é um problema, mas sairão ser afastar 25 quilómetros das cidades perceberá que ter acesso a uma conexão de fibra ótica não é tão simples e economicamente tende a ser consideravelmente mais caro.

Para poder tomar uma decisão sobre isto, precisamos conhecer os tipos de nuvens que existem e o tipo de serviços que podem ser contratados.

Tipos de nuvens

- Públicas:
- Aquelas que fornecem os provedores como a Altice, Amazon, Microsoft, Google, ...
- Toda a infraestrutura está nas suas instalações e outros é partilhada com outros clientes
- Privadas:
- Aquelas que adquiro e instalo em meus próprios CPDs para nos prestar o serviço. O problema é que estas são geralmente bastante caras.

- Híbridas:
- Em grandes ambientes corporativos, tanto públicos como privados, elas estão muito difundidas. Uma parte da infraestrutura mesmos é nossa e a outra parte é alugada a um provedor externo, objetivando-se assim redundância e tolerância a falhas.

Tipos de serviços:

- IaaS: Infrastructure as a Service.
- Com esse tipo de serviço, o que o fornecedor nos oferece são Máquinas Virtuais, nas quais poderemos colocar os nossos servidores, os nossos equipamentos de comunicações, os nossos sistemas de segurança, balanceadores de carga, ...
- SaaS: Software as a Service.
- Com este tipo de serviço, o que fornecemos aos nossos utilizadores é o Software (CRM, ERP, ...), escritórios virtuais, correio eletrónico na nuvem, ...
- PaaS: Platform as a Service.
- Com esse tipo de serviço, adquirimos plataformas como um serviço, para desdobramento de sistemas aplicacionais como servidores web, bases de dados, sistemas de big data, ...

Uma coisa que deve ficar clara é que a segurança dos serviços é geralmente compartilhada entre o fornecedor e o cliente. A administração, gestão e securitização destes ambientes devem ser contratadas além da contratação da infraestrutura. Isto advém da nossa vontade/interesse em usar uma infraestrutura na nuvem, mas sermos o seu gestor. Portanto, o provedor do serviço cloud poderá oferecer essa opção, passando a ser nossa a sua gestão ou então, em alternativa, externalizar para esse mesmo provedor a administração da nossa própria infraestrutura na nuvem.

2. RISCOS E AMEAÇAS.

Utilizar serviços na nuvem exige uma mudança de mentalidade, já que a nossa infraestrutura deixa de estar totalmente sob o nosso controlo, como acontecera até agora.
Embora já tenhamos mencionado as vantagens económicas, de flexibilidade e escalabilidade, de que podemos beneficiar ao utilizar os serviços cloud, nem tudo o que brilha é ouro, devemos ter em conta os riscos que assumimos e as ameaças as que estamos expostos:

- Geralmente, não temos acesso às instalações físicas dos nossos fornecedores cloud. No entanto, devemos conhecer a localização real das nossas máquinas virtuais.
- Devemos ter muito claros os contratos que garantem o nosso relacionamento e que deverão incluir:
    - Quais os serviços que são fornecidos.
    - Quais os tempos máximos de resposta.
    - As responsabilidades assumidas pelo fornecedor, exigindo cláusulas de confidencialidade e segurança de dados, já que devemos cumprir as leis de proteção de dados vigentes em cada momento.

Como indicámos anteriormente, uma perda de conectividade pode paralisar a atividade de minha empresa.

Teremos que manter as políticas de segurança que afetavam os serviços que deslocamos para a nuvem.

As ameaças estarão diretamente ligadas ao tipo de serviço contratado e ao contrato de serviços assinado, tendo um especial impacto quem deve encarregar-se de gerir e administrar os serviços.
Se não temos todos estes aspetos controlados, podemos ser afetados por:

- Fugas de informação.
- Usurpação de identidade.
- Acessos não autorizados.
- Incumprimento normativo.
- …

3. CONSIDERAÇÕES LEGAIS.

Se tivermos em conta a legislação vigente que nos afeta a todo o instante, então devemos levá-la em conta quando decidirmos contratar serviços em cloud.
Em Espanha, as empresas eram afetadas pela Lei Orgânica de Proteção de Dados (LOPD), mas desde 25 de maio último, regemo-nos pelo novo Regulamento Geral de Proteção de Dados (RGPD) Europeu, que visa unificar critérios respeitantes à proteção de dados pessoais, a nível europeu.
O RGPD é uma norma diretamente aplicável, que não requer normas internas de transposição nem, na maioria dos casos, normas de desenvolvimento ou aplicação. Portanto, os responsáveis devem antes de tudo assumir que a norma de referência é o RGPD e não as normas nacionais, com vinha acontecendo até agora.
Quanto aos serviços cloud, o principal aspeto que devemos ter em conta é que a localização dos nossos dados, ou seja, as máquinas em que armazenamos os nossos dados ou o nosso correio eletrónico devem estar no âmbito territorial permitido no RGPD.

A fim de cumprir as obrigações impostas pelo Regulamento Europeu, devemos considerar:

- A proteção desde o desenho e por defeito, não apenas com a obrigação de garantir a segurança dos dados pessoais, mas também a de ter em conta a forma de armazenamento usada para garantir o direito de acesso, de retificação e limitação de tratamento, o direito ao esquecimento e, sobretudo, o novo direito de portabilidade dos dados.
- Cumprimento proativo, dispondo de todas as medidas técnicas e organizativas apropriadas para poder demostrar, em qualquer momento, que os tratamentos de dados estão em conformidade com o presente Regulamento.

    - Em caso de manipulação de informação de carácter pessoal, o Regulamento exige que o fornecedor contratado ofereça garantias quanto ao cumprimento, isto é, que

disponha e possa demonstrar que conta com todos os meios necessários para cumprir suas obrigações, como encarregado na manipulação e tratamento dos dados pessoais do seu cliente. Para isso, o responsável dos dados pessoais não só deve assinar o contrato com o fornecedor de Cloud, onde se estabeleçam as suas obrigações no manejo dos dados, mas deverá estabelecer, no processo de seleção do fornecedor, mecanismos para poder determinar se este tem capacidade para assumir as garantias suficientes para o cumprimento do Regulamento e a proteção dos direitos dos interessados.

Avaliações de impacto para determinados tratamentos de dados, como na elaboração de perfis ou quando sejam manipulados dados de categoria especial em larga escala, que são os que dizem respeito à origem racial, religião, afiliação sindical, genéticos e de saúde. Isso determinará quais os riscos que podem existir no tratamento de dados pessoais.

- Relativamente às medidas de segurança a serem implementadas sobre os dados, estas devem ser ajustadas ao risco, e podem incluir pseudonimização e encriptação (tanto quando os dados estão em trânsito como quando estão armazenadas nos meus equipamentos informáticos), de forma a garantir a confidencialidade, integridade, resiliência dos sistemas e serviços, capacidade de restaurar a disponibilidade e o acesso aos dados rapidamente. Mas os riscos para a pessoa responsável pelos dados e a empresa que fornece o serviço cloud podem não ser os mesmos, dado que esses riscos vão depender dos tratamentos de dados realizados por cada um deles. Portanto, será conveniente acordar, no âmbito do contrato de prestação de serviço com o fornecedor, quais serão esses riscos e as medidas que devem ser implementadas.
    - No caso de acontecer uma violação de segurança nos dados, e se houver um risco para os direitos e liberdades das pessoas, é obrigatório notificar este incidente à Comissão Nacional de Proteção de Dados (CNPD), no prazo de 72 horas após ter tido conhecimento.
    - Devemos ter claro quem é o responsável pelo incidente, o fornecedor ou nós. Se a lacuna de segurança for atribuível ao fornecedor do serviço cloud, ele deverá notificar-nos sobre esta falha, para posteriormente podermos notificar a CNPD. Para cumprir com esta obrigação, deveremos estabelecer um procedimento que determine quais violações de segurança que serão notificadas e os mecanismos de notificação.

Deveremos informar, inclusivamente, os interessados, quando os seus dados sofreram um risco elevado do ponto de vista dos seus direitos e liberdades, tendo então que complementar o procedimento de notificação de violações de segurança à CNPD com um mecanismo que permita comunicar a ocorrência às pessoas.

CAPÍTULO 3. ESTÁ PREPARADO PARA UM CIBERATAQUE?

1. INFECÇÃO POR RANSOMWARE.

1.1. O QUE É O RANSOMWARE?

O Ransomware é um Malware (software malicioso) que bloqueia o nosso dispositivo, podendo chegar a encriptar o conteúdo do disco rígido. Uma vez perdido o controlo sobre os nossos equipamentos, somos obrigados a pagar um resgate que geralmente é solicitado em criptomoedas, bitcoins, por exemplo.

Hoje existe Ransonware tanto para equipamentos de mesa e portáteis como para dispositivos móveis (smartphones e tablets).

O Ransomware chega escondido dentro de um ficheiro ou programa e é ativado quando executamos o arquivo ou programa.

Podemos ser infetados a partir de ficheiros que recebemos como anexos em correios eletrónicos ou que recebemos como anexos em aplicações de mensagens instantâneas, como WhatsApp ou Telegram. Esta situação tanto pode ocorrer em dispositivos móveis como em computadores de escritório ou portáteis se utilizarmos aplicações web que nos permitem utilizar os referidos serviços nesses dispositivos.

Também podemos ser infetados visitando páginas de origem duvidosa: pornográficas ou fazendo download de filmes ou música e, inclusive, realizando o processo de atualização de sistemas operativos e softwares legítimos, como Microsoft Windows ou Adobe Flash se não o fizemos através dos websites oficiais dos fabricantes.

Depois de penetrar no computador, o malware é ativado e provoca o bloqueio de todo o sistema operativo enviando uma mensagem de aviso com a ameaça e o montante do "resgate" que deve ser pago para recuperar toda a informação. A mensagem pode variar em função do tipo de ransomware que enfrentemos: conteúdo pirateado, pornografia, vírus falsos, ...

1.2. COMO EVITAMOS SER INFECTADOS?

Para evitar ser infetado por um Ransonware, devemos seguir as seguintes indicações de bom senso:

- Manter o nosso sistema operativo e as nossas aplicações atualizadas, evitando assim que o atacante aproveite as vulnerabilidades já identificadas.
- Ter, pelo menos, um antivírus sempre atualizado.
- Não abrir e-mails ou ficheiros com remetentes desconhecidos. Irão constantemente tentar enganar-nos enviando-nos e-mails com um “isco” para nós “mordermos”.
- Evitar navegar em páginas inseguras ou com conteúdo não verificado.
- Ter um sistema de cópias de seguranças e um procedimento de recuperação definido que nos permitirá recuperar o sistema no menor tempo possível sem perda de informação.

1.3. UMA VEZ INFECTADOS, COMO RESOLVÊ-LO?

Bem, isto realmente não é simples. As autoridades e o próprio INCIBE insistem em não pagar o resgate porque ninguém garante a recuperação do acesso à informação. Por outro lado, embora você a recupere é quase certo que os seus equipamentos ficarão infetados com algum outro tipo de malware.

A melhor solução seria recuperar uma cópia de segurança, o mais recente possível, mas muitas vezes não a temos.

Noutros momentos e se o ransomware já estiver identificado e analisado, é possível que exista algum tipo de procedimento de recuperação.

Caso contrário, podemos recorrer a:

- O serviço antiransomware do INCIBE
  https://www.incibe.es/en/node/5139
- O grupo de crimes telemáticos da Guardia Civil
  https://www.gdt.guardiacivil.es/webgdt/home_alerta.php
- A Brigada de Investigação Tecnológica (BIT) da Polícia Nacional.
  http://www.policia.es/org_central/judicial/udef/bit_alertas.html
- A Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T).
  https://www.policiajudiciaria.pt/unc3t/

1.4. COMPORTAMENTO DO RANSOMWARE AO INFECTAR O SISTEMA.

Durante estes últimos anos, sofremos inúmeros ataques do tipo ransomware e podemos qualificar os ataques de:

1. Bloqueio do sistema. "Vírus da Polícia".
1. Encriptação de Informação. CTB-Locker.
2. Bloqueio e encriptação do sistema. Segunda variante de Petya | Bad Rabbit.
3. Bloqueio e malware que comunica o resgate. Jisut.
4. Encriptação e roubo de informação ou carteiras virtuais. Cerber.
5. Ransomware PUBG. MSIL / Filedecoder.HD
6. Pagamento com fotos íntimas. nRansom.
7. Ransomware em dispositivos IoT
8. Ransomware em smartphones ou tablets.
9. Ransomware para fugas de informação.

2. ATAQUE POR PHISHING.

2.1. O QUE É PHISING?

Alguma vez já recebeu um e-mail de alguém pedindo para clicar num link que o direciona para uma página web na qual precisa de realizar algum tipo de revisão relativa aos seus dados pessoais? Muito cuidado! É muito possível que esteja a ser vítima de um ataque de phishing.

Phishing é uma técnica utilizada por cibercriminosos para, fazendo-se passar por uma entidade ou pessoa de confiança, através do correio eletrónico ou outros canais de comunicação, nos roubar informação confidencial, como nomes de utilizador, senhas e dados de cartões de crédito, entre outras coisas, enquanto acedemos a um serviço web que consideramos seguro e legítimo.

Embora vejamos phishing noutros cenários, o mais frequente está relacionado com a clonagem de uma página web para fazer o visitante acreditar que está no sítio web ao qual queria aceder, quando na verdade este é falso.

O utilizador acreditará que está acedendo a uma página web legítima e inserirá as suas credenciais de acesso sem perceber que na realidade está a enviar os seus dados para o atacante. Depois dos dados serem inseridos, e novamente sem perceber, será redirecionado automaticamente para a página legítima a que queria aceder.

A consequência é que os utilizadores não estão cientes de que o sítio web no qual estão inserindo informação confidencial é controlado por estes cibercriminosos.

Phishing é a origem de 90% dos ciberataques. É por isso que o investimento na consciencialização para preveni-los tem que ser cada vez mais elevada, sem esquecer que os cibercriminosos procurarão novos métodos de engano.

2.2. TIPOS DE PHISHING.

- **DECEPTIVE PHISHING**: é o mais comum e já descrito acima. Procura obter nossas credenciais para aceder a um serviço web (utilizador e senha, geralmente).
  Por exemplo: tentativa de phishing com o Carrefour.

F*onte: Guardia Civil*

- **MALWARE-BASED PHISHING**: são aqueles ataques em que o cibercriminoso espera que o utilizador faça download ou execute ou determinado ficheiro ou visite uma uma página web e com isso seja infetado por um Malware.
- **DNS-BASED PHISHING** Também conhecido como Pharming. O ataque consiste em modificar os ficheiros hosts de uma empresa ou o sistema de nomes de domínio da mesma, para que os pedidos de URL devolvam um endereço falso e as comunicações sejam dirigidas para um sítio web falso. Este tipo de ataques poderia ser atenuado se as senhas dos administradores dos routers que nos fornecem serviço à internet fossem alteradas aquando da sua instalação, algo que, no ambiente das PME, microempresas ou profissionais liberais, praticamente ninguém faz.
- **CONTENT-INJECTION PHISHING:** nestes ataques parte do conteúdo de um website legítimo é substituído com conteúdo falso desenhado para enganar ou desviar o utilizador e fazer com que este forneça a sua informação confidencial.
- **SEARCH ENGINE PHISHING:** por meio desta técnica podemos ser alvo de uma infeção por simplesmente fazer uma pesquisa no Google ou Bing, uma vez que esses links maliciosos são indexados nos motores de busca dos próprios motores de pesquisa, surgindo assim como resultados válidos numa pesquisa comum. Um dos casos mais memoráveis foi o sofrido pelo Banco Sabadell. Durante um período de tempo, dois anúncios patrocinados apareceram nas duas primeiras posições dos resultados de pesquisa do Google. Quando se clicava neles, a vítima era redirecionada para uma página web fraudulenta que era diferente da oficial no URL.
- **MAN-IN-THE-PHISHING:** é o mais difícil de detetar, pois o cibercriminoso coloca-se entre o computador do utilizador e o servidor, registado assim a informação que é transmitida entre os dois.

2.3. COMO PODEMOS EVITAR O PHISHING?

- Não responda a nenhum e-mail que solicite informação pessoal ou financeira. Lembre-se que nenhum banco ou outras entidades solicitam informação confidencial através de canais não seguros e, em nenhum caso, o fazem por correio eletrónico.
- Nunca clique num link que o convidem a visitar. Em qualquer caso, escreva você mesmo o endereço no seu navegador da Internet.
- Verifique se a página utiliza o protocolo HTTPS para proteger a autenticação e a comunicação. Um pequeno cadeado aparecerá nos navegadores. Se o endereço começar com http://, não continue.
- Ative junto do seu banco o sistema, disponível em quase todos, que obriga a que quando uma transferência for feita a partir das suas contas você seja notificado.
- Use sistemas antisspam.

3. FUGA DE INFORMAÇÃO.

Em 2010 ocorreu, a que é considerada até hoje, a maior fuga de informação da história. WikiLeaks, uma organização sem fins lucrativos publicou um total de 250.000 documentos que foram enviados entre o Departamento de Estado dos Estados Unidos e suas embaixadas espalhadas por todo o mundo. As consequências são conhecidas de todos.

Todos os incidentes de fuga de informação mostram-nos como é difícil proteger a confidencialidade da informação, por outro lado, o ativo mais valioso de qualquer organização.

Nós denominamos incidentes de **fuga de informação** àqueles incidentes que colocam em poder de uma pessoa alheia à organização, informação confidencial. O incidente pode ser interno ou externo e pode ser provocado ou não intencional.

Alguns exemplos de fuga de informação podem ser:

- Um empregado vendendo informação confidencial concorrência concorrentes (incidente interno e intencional).
- Um administrativo que perde um documento num local público (incidente interno e não intencional).
- A perda de um portátil, tablet, smarphone ou *pendrive* (incidente interno e não intencional).
- Acesso, desde o exterior, a uma base de dados da organização (incidente externo e intencional).
- Um equipamento infetado com um Spyware que envie informação para o exterior sem que estejamos cientes desta situação (incidente externo e intencional).

A intencionalidade do incidente determina o impacto da fuga de informação. No caso do incidente não ser intencional, é muito provável que não ocorra nada; no entanto, nos incidentes provocados, o impacto é evidente e vai depender do tipo de informação que foi afetado. Independentemente de a origem ser ou não intencional, a realidade é que o incidente é dificilmente reparável, podendo levar a perdas económicas e até a perdas de reputação ou de imagem.

Impacto global

- Dano de imagem.
- Consequências legais.
- Consequências económicas.
- Outras consequências que implicam um impacto negativo em âmbitos muito diversos, como, por exemplo, o âmbito institucional, político, diplomático ou governamental, entre outros.

Outros fatores a ter em consideração, sobre o impacto global, tem a ver com o tipo de informação que foi roubado:

- Se são dados pessoais ou não.
- Se os dados são internos ou externos à organização.

4. ATAQUE POR ENGENHARIA SOCIAL.

A Engenharia social, que não é outra coisa que conseguir enganar alguém a fim de obter dessa pessoa o que se deseje, tornou-se um dos principais vetores de ataque às empresas. Principalmente porque a partir deste ataque, tipicamente feito a um trabalhador, se podem iniciar ataques como os descritos acima: malware, ransomware, ..., chegando inclusive às temidas APTs ou Ameaças Avançadas Persistentes.

O termo tornou-se famoso após a publicação, pelo "The New York Times", do ataque realizado por uma unidade militar chinesa (conhecida como APT1) contra as redes de diferentes meios de comunicação, através de uma campanha de spearphishing e malware.

As APTs são, provavelmente, o ataque mais sofisticado que podemos encontrar e ao qual o cibercriminoso vai destinar mais recursos. A diferença do visto até agora é que estes são ataques dirigidos contra empresas específicas e não ataques genéricos.

CAPÍTULO 4. RELAÇÃO SEGURA COM FORNECEDORES E CLIENTES.

1. INTRODUÇÃO.

Todas as empresas precisam de interagir com os seus fornecedores e clientes para que a atividade que desenvolvem gere os benefícios desejados.

Relativamente aos nossos clientes, em primeiro lugar, devemos cumprir com a legislação vigente, RGPD, para garantir que os dados que armazenamos estão num lugar seguro e longe do alcance de um cibercriminoso.

Além dos dados pessoais, praticamente todo o nosso relacionamento com os nossos clientes já é digital. Encomendas, notas de entrega, faturas, relatórios, ..., são enviados por correio eletrónico, usamos ferramentas de mensagens instantâneas como o WhatsApp ou Telegram, ou armazenamos a informação que queremos enviar num espaço na nuvem, como o Drive da Google, a Onedrive da Microsoft, a Dropbox, ... enviando-lhes o link de acesso aos mesmos.

É fundamental que os nossos clientes confiem em nós, e não apenas em relação aos serviços que nos contratam, mas também relativamente ao tratamento que fazemos da sua informação. Por outro lado, é já muito frequente que os nossos grandes clientes nos obriguem a implementar medidas de segurança tecnológica que garantam que não irão surgir problemas causados por umas deficientes medidas de segurança tecnológica da nossa parte e que os possam prejudicar.

No que diz respeito aos nossos fornecedores, estamos numa posição idêntica aquela que os nossos clientes têm connosco. Neste caso é preciso exigir a mesma coisa que nos é exigido aquando do relacionamento com os nossos clientes: medidas de segurança informática suficientes e um tratamento dos nossos dados em conformidade com a legislação em vigor.

Todas as empresas contratam serviços a terceiros, principalmente porque não podem contratar um especialista em todas as áreas necessárias para gerir a atividade empresarial.

Por exemplo:

- Assessoria laboral, jurídica ou fiscal.
- O fornecedor de informática: sistemas / comunicações internas, copiadoras, ...
- O fornecedor de comunicações: voz, dados e internet.
- E dependendo da nossa atividade, vamos interagir com muitos outros fornecedores.

Por outro lado, é cada vez mais comum contratar serviços cloud para armazenar as nossas máquinas ou os nossos dados. Dependendo do tipo de contratação que fizermos, apenas a infraestrutura ou fornecimento de um serviço completo de gestão e administração, deveremos exigir dos nossos fornecedores, por meio de um contrato, que cumpram a lei e que tenham implementadas as medidas de segurança necessárias para garantir a nossa atividade ou para recuperá-la em caso de um incidente.

Com todos eles, clientes e fornecedores, devemo-nos sentar para discutir os termos da nossa relação e como nos afeta mutuamente a tecnologia com a qual comunicamos, para garantir que não surgem problemas operacionais ou legais para ambas as partes.

No que diz respeito ao cumprimento legal ou legislativo que comentámos anteriormente, no passado dia 25 de maio começou-se a aplicar o Regulamento Geral de Proteção de Dados europeu, que já estava em vigor desde 27 de abril de 2016. Este novo regulamento tem um impacto especial

nas relações que temos com os nossos fornecedores e clientes e vem unificar os critérios em todos os estados membros, praticamente substituindo os regulamentos nacionais que estavam em vigor em cada estado. No caso espanhol, a Lei Orgânica de Proteção de Dados (LOPD).
Segundo os últimos relatórios publicados, 65% das empresas não estão preparadas para cumprir o RGPD, embora tenham tido dois anos para se adaptar.
Por que deve cumprir o RGPD?

- Em primeiro lugar, porque é de cumprimento obrigatório, independentemente do tamanho da empresa.
- Em segundo lugar, porque as sanções podem atingir 4% da nossa faturação, em casos muito graves.
- Em terceiro lugar, porque não posso exigir que um cliente ou provedor proteja a minha informação se eu não me preocupo em proteger a sua.
- Em quarto lugar, porque em 10 de abril, a Agência Espanhola de Proteção de Dados informou que tinha aberto a sua sede eletrónica para que as empresas e as instituições públicas, obrigatoriamente, informassem quem seria o seu Encarregado da Proteção de Dados.
- Em quinto lugar, porque a implementação das medidas de segurança ativa propostas pelo regulamento fará com que trabalhemos de maneira mais segura, minimizando o risco de sofrer um incidente ou um ciberincidente.

Não se esqueça: A proteção de dados pessoais de acordo com o RGPD não serve apenas para evitar sanções, serve para obter uma vantagem competitiva face à concorrência.

Evidentemente, há uma importante diferença entre uma grande empresa e uma PME na hora de implementar as medidas exigidas, no entanto, como já dissemos antes, é de cumprimento obrigatório para todos e, enquanto as grandes empresas há anos que estão a tratar os dados conforme a lei, de forma global as PME ainda estão a anos-luz no que diz respeito ao cumprimento do RGPD. Como dizem alguns, não estão maduras. E o problema é que teremos que amadurecer a uma velocidade vertiginosa.

O ponto de viragem ocorrerá no momento em que as empresas começarem a ser sancionadas.

A própria diretora da Agência Espanhola para a Proteção de Dados, **Mar Espanha**, deixou claro nos seus recentes discursos, indicando que não haverá nenhum tipo de moratória a este respeito, portanto, a partir de 25 de maio, todas as organizações devem cumprir com o Regulamento e estar em condições de demonstrá-lo. Além disso, indicou que os planos de inspeção da Agência incidirão sobre três sectores específicos: saúde, instituições financeiras e empresas de telecomunicações, começando imediatamente na data de aplicação obrigatória, ou seja, a partir de 25 de maio.

2. RISCOS NO RELACIONAMENTO COM FORNECEDORES.

Temos de ter em conta que, em Espanha, um país em que mais de 95% das empresas são PME, e destas numa percentagem semelhante são microempresas e profissionais independentes,

normalmente temos uma economia de pequenas empresas que prestam serviços a empresas pequenas.
Este modelo económico causa problemas especialmente nas épocas de crises como as que estamos a sofrer (digo "a sofrer" porque ainda existem muitas empresas que não superaram a crise), pela impossibilidade de manter os quadros, o que afeta negativamente os serviços que fornecemos ou nos são fornecidos.
A gestão de riscos permite controlar a incerteza que afeta uma ameaça. Para isso, identificamos, avaliamos e tratamos esses riscos e avaliamos o impacto da exposição a uma ameaça, juntamente com a probabilidade desta se materializar.
Para evitar riscos, devemos estar muito atentos a se os serviços que contratámos são recebidos com um nível de qualidade suficiente. É preciso avaliar os nossos fornecedores periodicamente, dado que uma parte importante do nosso sucesso depende diretamente deles.
Portanto, devemo-nos acostumar a gerir os fornecedores além da assinatura do contrato:

- Se um contrato padrão não se adequa às nossas necessidades, devemos negociar contratos e SLAs (contratos de nível de serviço) alinhados com os nossos interesses e necessidades.
- Avaliar o serviço que recebemos periodicamente, para:
    - Minimizar os riscos de segurança evitando assim:
        - Por um lado, sanções.
        - Por outro lado, que sejamos incapazes de fornecer os nossos serviços, o que provocaria, além de perdas económicas, que a nossa reputação e imagem sejam afetadas face aos nossos clientes.
    - Evitar roubos ou fugas de informação.
    - Ter a capacidade de resposta necessária naqueles excessos pontuais de necessidade de trabalho.

Quando os nossos serviços são suportados por fornecedores cloud, devemos assegurar-nos de que cumprem a lei e implementam medidas de segurança ativa: segurança física e lógica, backups, monitorização dos seus sistemas, ...

Tenha em mente que, apesar de ter alugado a infraestrutura, é responsável pela sua segurança, especialmente porque a gere, ou porque terceirizou a gestão num fornecedor, caso em que deve estar vigilante para que o fornecedor cumpra os seus contratos e SLAs e não cause qualquer um dos prejuízos que já mencionámos. Portanto:

- Devemos definir as nossas medidas de segurança e os riscos que somos capazes de assumir e os que devemos evitar.
- Sempre que for possível, devemos conhecer as instalações de onde o serviço nos vai ser fornecido.
- Devemos exigir que nos enviem periodicamente relatórios nos quais seja feita referência à eficácia dos controlos implementados.

3. ACORDOS COM FORNECEDORES E COLABORADORES.

Precisamos de integrar os nossos fornecedores no desenvolvimento das nossas operações. Uma estreita colaboração com os nossos fornecedores irá permitir minimizar riscos e otimizar custos e prazos. Para isso, utilizaremos quatro diretrizes básicas que nos permitam definir a relação e reforçar a estratégia:

- Externalização dos serviços que não estão no core do nosso negócio.
- Estar rodeados dos melhores permitir-nos-á ser melhores e estar mais perto de alcançar a tão esperada diferença competitiva para com a nossa concorrência.
- Sempre que possível, é melhor ter o fornecedor perto. A colaboração tende a tornar-se mais estreita.
- Integração dos fornecedores nas nossas operações diárias. Envolvê-los nos nossos dispositivos permitirá gerar sinergias benéficas para ambas as partes.

Por outro lado, como indicado acima, não devemos conformar-nos com um acordo padrão se ele não se adequar às nossas necessidades. Nestes contratos, devemos incluir cláusulas que façam referência a:

- Acordos de confidencialidade, ou seja, o compromisso que o fornecedor deve assumir de não divulgar a informação a que tenha tido acesso durante a prestação do seu serviço, e inclusive exigir-lhes cláusulas de Propriedade Intelectual, se for necessário.
- Que a informação esteja encriptada, encontrando-se esta nos seus equipamentos ou estando em trânsito. Esta é uma exigência do novo RGPD para empresas de determinados setores.
- Proteção de dados pessoais.
- Penalizações por incumprimento de contrato.

4. USO SEGURO E RESPONSÁVEL DO CORREIO ELETRÓNICO E SERVIÇOS DE MENSAGENS INSTANTÂNEAS.

Como indicado na introdução, praticamente toda a nossa relação com os nossos fornecedores e clientes é digital.
Para comunicarmos com eles, utilizamos tanto o correio eletrónico como ferramentas de mensagens instantâneas, como o WhatsApp.
Precisamente 3 serviços vulneráveis e geralmente utilizados para nos atacarem do exterior. Provavelmente, atualmente, são o principal vetor de ataque, já que tal como a comunicação evoluiu de um correio postal tradicional para mensagens eletrónicas, as fraudes e os enganos também o fizeram, aproveitando-se agora de utilizadores ingénuos ou com escassa consciencialização sobre cibersegurança.
Em todos os casos devemos utilizar diferentes serviços no âmbito pessoal e profissional. Misturar estes âmbitos pode criar mais do que uma dor de cabeça.
Tipos de problemas que se aproveitam destas tecnologias:

- Hoax ou notícias falsas.

- Fraudes.
- *Spam*: **mensagens massivas, anónimas e indesejadas.**
- Phising.
- Distribuição de Malware.
- E um amplíssimo etc ...

Em relação ao uso do correio eletrónico como meio de transmissão de campanhas de e-mail marketing, é preciso ter muito cuidado:

- Em primeiro lugar, normalmente têm um desempenho muito baixo porque a maioria das pessoas não lê e-mails publicitários.
- Em segundo lugar, porque o nosso endereço de correio eletrónico poderia ser considerado spam e isso poderia provocar que nosso e-mail não chegue aos seus destinatários sendo bloqueado pelos filtros anti-spam:
    - Filtros Bayesianos.
    - Listas negras.
    - Filtros challenge / response.
    - Filtros firewalls.
    - Filtros baseados na reputação do domínio de onde são enviados.
    - …

Há relatórios que dizem que mais de 75% do correio que é enviado diariamente é spam. Levando em conta a gravidade do assunto e a facilidade com que o spam nos pode nos causar Problemas sérios, não deixam de surgir ferramentas para combatê-lo. Uma das mais utilizadas é o “spam scores”, um dos mais poderosos testes de spam do momento.

Os filtros anti-spam condicionam o spam score e podem forçar a detenção de um e-mail antes deste chegar ao seu destinatário, se o índice atribuído às nossas mensagens for alto ou forem marcados como maliciosos.

Isto pode causar um problema muito sério, visto que poderia impedir que comunicássemos por correio eletrónico durante uma temporada, e difícil de resolver a curto prazo.

Para envios massivos, são utilizados outros sistemas.

Por outro lado, uma boa consciencialização do nosso pessoal sobre o uso correto destas ferramentas de comunicação irá permitir evitar que os cibercriminosos os usem para nos prejudicar:

- Devemos ser capazes de identificar e-mails maliciosos.
- Não nos devemos deixar enganar por phishing.
- Não devemos responder mensagens que possam ser spam ou clicar em links que desconheçamos.
- Não fazer download de ficheiros anexos recebidos de endereços de e-mail desconhecidos.
- Utilizar senhas seguras e alterá-las com regularidade.
- Não enviar e-mails em cadeia.

- Usar sistemas de segurança como antivírus e antisspam para o correio eletrónico.
- Em síntese, usar o bom senso.

Em relação às ferramentas de mensagens instantâneas, também é preciso ter muito cuidado. Os nossos smartphones podem ser infetados de uma forma muito simples, enviando imagens ou ficheiros que recebemos, sobretudo, pelo WhatsApp. Uma vez infetado o smartphone, não vamos tardar muito em ligá-lo ao computador ou portátil para carregar porque está a ficar sem bateria e, nesse momento, o computador será também infetado.

Para efeitos da regulamentação de proteção de dados, o Grupo de Trabalho do artigo 29 (GT 29) chegou à conclusão, através de uma carta emitida no passado mês de outubro de 2017, que o Whatsapp não pode obter o consentimento dos utilizadores através de uma caixa já selecionada por defeito, para ceder os nossos dados pessoais ao Facebook. Isto é, devido à ambiguidade dos termos e condições que utiliza, que fazem com que a forma de dar o necessário “consentimento” seja totalmente contrária à definida no novo Regulamento Geral de Proteção de Dados (RGPD).

Poderíamos dizer que o WhatsApp ignorou tudo o que tem a ver com uma "manifestação de vontade, livre, inequívoca, específica e informada". Não só porque a dita caixa de confirmação aparece pré-marcada, mas porque não somos informados sobre os dados pessoais que serão cedidos nem o seu propósito.

Em síntese, para as autoridades de controlo de proteção de dados, o WhatsApp não cumpre os requisitos de consentimento e de legítimo interesse na transmissão de dados ao Facebook com a sua política de "take it or leave it" ("pegar ou largar "). O GT29 é constituído por um representante da autoridade de proteção de dados de cada Estado-Membro da União Europeia, a Autoridade Europeia para a Proteção de Dados e a Comissão Europeia.

PARCEIROS DO PROJETO

Associação Empresarial do Alto Tâmega (ACISAT) *http://acisat.pt*

Câmara de Comercio de Zamora *http://www.camarazamora.com/*

Instituto Politécnico de Bragança (IPB) *https://portal3.ipb.pt/index.php/pt*

Diputación de Ávila https://www.diputacionavila.es/

MAIS INFORMAÇÕES SOBRE O PROJETO COMPETIC E AS SUAS ATIVIDADES

Web: http://competic-poctep.com

E-mail: info@competic-poctep.com

Parque Tecnológico de Boecillo

C / Luis Proust 17 47151 Boecillo - Valladolid