Presidência do Governo Regional dos Açores
Direção Regional das Comunicações e da Transição Digital

MANUAL DE BOAS PRÁTICAS DE CIBERSEGURANÇA PARA OS ORGANISMOS DO PODER LOCAL

Presidência do Governo Regional dos Açores
Direção Regional das Comunicações e da Transição Digital

MANUAL DE BOAS PRÁTICAS DE CIBERSEGURANÇA PARA OS ORGANISMOS DO PODER LOCAL

Manual de Boas Práticas de Cibersegurança para os Organismos e Poder Local

Presidência do Governo dos Açores, através da Direção Regional das Comunicações e da Transição Digital.

Tiragem:
500 exemplares

Local de Impressão:
São Miguel, Açores

Data:
Julho de 2023

Mensagem

O digital é para o quotidiano das atuais gerações e futuras uma essência de comunicação, como foi também no passado, para as gerações que nos antecederam a energia elétrica para a economia geral e conforto.

A nossa era digital, com a disseminação das novas tecnologias, é uma oportunidade para reinventarmos, diariamente, a forma como interagimos, tirando o melhor partido do desenvolvimento das ferramentas tecnológicas, que rentabilizam todas as atividades afetas à nossa vida pessoal e profissional.

Esta disrupção tecnológica já trouxe e traz, cada vez mais, tanto vantagens, como preocupações, associadas à, agora, velocidade vertiginosa das alterações no campo tecnológico, que impõem familiarização com a modernização constante de conteúdos substantivos e supostamente consolidados, pondo assim em causa a preservação da segurança da utilização desses mesmos meios.

A necessidade de garantirmos a segurança da informação que detemos e das infraestruturas que a sustentam deve constituir um alerta e transformar-se numa prioridade para todos nós. É, então, necessária uma adaptação a esta nova realidade, onde os ciberataques têm vindo a crescer em número e sofisticação, atingindo todos os setores de atividade económica e a administração pública.

O digital é para o quotidiano das atuais gerações e futuras uma essência de comunicação, como foi também no passado, para as gerações que nos antecederam a energia elétrica para a economia geral e conforto.
A nossa era digital, com a disseminação das novas tecnologias, é uma oportunidade para reinventarmos, diariamente, a forma como interagimos, tirando o melhor partido do desenvolvimento das ferramentas tecnológicas, que rentabilizam todas as atividades afetas à nossa vida pessoal e profissional.
Esta disrupção tecnológica já trouxe e traz, cada vez mais, tanto vantagens, como preocupações, associadas à, agora, velocidade vertiginosa das alterações no campo tecnológico, que impõem familiarização com a modernização constante de conteúdos substantivos e supostamente consolidados, pondo assim em causa a preservação da segurança da utilização desses mesmos meios.
A necessidade de garantirmos a segurança da informação que detemos e das infraestruturas que a sustentam deve constituir um alerta e transformar-se numa prioridade para todos nós. É, então, necessária uma adaptação a esta nova realidade, onde os ciberataques têm vindo a crescer em número e sofisticação, atingindo todos os setores de atividade económica e a administração pública.
Neste sentido, não temos dúvidas, a prevenção é a melhor forma de mitigar os riscos e impactos decorrentes de incidentes no ciberespaço. Neste enquadramento, o XIII Governo Regional dos Açores, consciente dos riscos existentes no mundo cibernético, assume através de um conjunto de recomendações e de boas práticas de cibersegurança, que importa sensibilizar todos os utilizadores para a adoção de condutas que promovam comportamentos preventivos e responsáveis, mitigando, possíveis riscos e impactos decorrentes dos incidentes no ciberespaço, ligados aos dados, à tecnologia e às infraestruturas.
O Programa do XIII Governo Regional dos Açores foi o primeiro a abordar a cibersegurança, e entretanto o Governo já executou, em 2022, um investimento de dois milhões de euros nesta área. No âmbito do Plano de Recuperação e Resiliência (PRR), assegurámos o apoio ao Azores Cyber 360º, assumindo, através dele, que a cibersegurança é um dos pilares de desenvolvimento futuro do nosso território, e visto que consolida o nosso posicionamento de vanguarda ao nível da Inovação e Desenvolvimento Tecnológico.

ÍNDICE GERAL

1. Introdução

O presente manual descreve um conjunto de recomendações e boas práticas de cibersegurança que podem ser adotadas pelos Organismos do Poder Local (OPL) da Região Autónoma dos Açores, como forma de atenuar significativamente os riscos cibernéticos.

Os organismos da Administração Pública, a todos os níveis – e as funções e serviços que desempenham em prol dos cidadãos e organizações – são a pedra angular da nossa sociedade. É a sua própria essencialidade, contudo, que os torna particularmente atraentes para um exército de cibercriminosos. Estes colocam ameaças crescentes e detêm frequentemente o tipo de cibercapacidades poderosas que, até há bem pouco tempo, estariam ao alcance apenas dos Estados.

Seja em busca de dados institucionais para ganharem vantagens estratégicas ou procurando perturbar a boa entrega de serviços públicos para obter ganhos financeiros ou políticos, certo é que a ameaça enfrentada pela Administração Pública, também no Poder Local, é bem real e presente.

Na defesa contra estes ataques, é da maior importância o conhecimento e as atitudes dos agentes e funcionários da Administração Pública.

Ainda que para mitigar os riscos ligados à cibersegurança seja necessário adotar tecnologias avançadas e outros instrumentos organizacionais eficazes, isso nada retira ao papel essencial que cada indivíduo desempenha. Cada um de nós tem um contributo crítico a fazer para o sucesso e robustez do ecossistema da segurança da informação e da cibersegurança da Administração Pública Regional (APR).

É impossível garantir que, se seguir todas as regras e recomendações constantes deste manual, estará o organismo totalmente livre de ataques. No entanto, estaremos garantidamente muito mais protegidos, se todos fizermos a parte que nos cabe e em muito melhores condições para respondermos com maior rapidez e eficácia a qualquer incidente com o qual nos possamos deparar.

2. Modelo de Governança

A governança, neste contexto, refere-se ao conjunto de atividades que permite às organizações tomarem decisões de cibersegurança sólidas. As etapas delineadas neste capítulo fornecem uma visão geral das atividades de governança, tais como definir os princípios de um programa de cibersegurança, fornecer uma visão holística do risco e monitorizar ativamente o desempenho.
Uma governança de cibersegurança claramente definida permite que as organizações maximizem os benefícios de operar numa economia digital. Uma governança eficaz da cibersegurança apoiará o sucesso e a sustentabilidade da transformação e da transição digital na Organismo ou Freguesia. A governança da cibersegurança poderá ser assegurada em seis etapas distintas.

Etapa 1 - Construção de uma Cultura de Cibersegurança

O Organismo do Poder Local (OPL) deve desenvolver uma cultura de resiliência cibernética, num contexto em que todos, na organização, se sintam apoiados para tomar decisões que protejam a confidencialidade, integridade e disponibilidade de ativos e sistemas de informação. A sensibilização e a responsabilidade pela resiliência cibernética devem ser encaradas em toda a organização como uma parte importante e complementar da missão do Poder Local.
O estabelecimento da cultura de cibersegurança de uma organização deve ocorrer sobretudo de cima para baixo. A gestão de topo deve demonstrar um compromisso com a resiliência cibernética. Isto pode ser comunicado e reforçado através de estratégias, políticas e normas.

Etapa 2 - Estabelecimento de funções e responsabilidades

Definir claramente os papéis e responsabilidades de cibersegurança no OPL e estabelecer quem é o mais indicado para executá-las é o segundo passo para alcançar uma governação eficaz da segurança cibernética.
O número de funcionários em organizações mais pequenas pode dificultar a separação dos deveres, sendo que as responsabilidades de cibersegurança podem recair sobre uma única pessoa. Em todos os casos, continua a ser importante assegurar que os deveres sejam realistas, claramente compreendidos e bem comunicados.

Etapa 3 - Gestão holística dos riscos

A cibersegurança apoiará a resiliência de um vasto leque de processos autárquicos. Por conseguinte, o risco é melhor considerado a nível holístico, onde as interdependências dos processos podem ser compreendidas. Na maioria das organizações, podem já existir quadros de gestão de riscos para áreas como a saúde e a segurança. O risco de cibersegurança deve alinhar-se com estes quadros existentes. O alinhamento permite a consistência da gestão de riscos, mas também enquadra a segurança cibernética de uma forma familiar para a organização mais ampla.
Uma gestão consistente dos riscos de cibersegurança de uma organização requer planeamento e preparação. O OPL deve ter uma boa compreensão dos seus principais ativos institucionais e das consequências para a sua atividade se a confidencialidade, integridade ou disponibilidade desses ativos estiver comprometida.

Etapa 4 - Colaboração na cibersegurança

A tradução com êxito de uma estratégia e visão de cibersegurança em ação requer o apoio da organização mais ampla. Isto pode ser conseguido através da criação de um comité e de um grupo de trabalho que contenha as principais partes interessadas de todo o negócio.
Um comité de direção deve incluir representantes que possam tomar decisões sobre que recursos devem ser priorizados e sobre as direções

a tomar no domínio da cibersegurança. O principal objetivo do comité de direção é alcançar um consenso e alinhar as prioridades de cibersegurança, riscos, iniciativas e relançamento dos objetivos do organismo.

Etapa 5 - Criar um programa de cibersegurança

O objetivo de um programa de cibersegurança é garantir que qualquer investimento em cibersegurança proporcione a melhor melhoria possível na resiliência cibernética, tal como definida pela estratégia.
Uma função fundamental do programa de segurança é a gestão do ciclo de vida de quaisquer tecnologias de cibersegurança implementadas. Sem manutenção, os sistemas e as capacidades perderão rapidamente a sua eficácia e poderão não fornecer os resultados pretendidos.

Etapa 6 - Medição da resiliência da cibersegurança

A medição e o reporte são a base para uma melhoria contínua do programa de cibersegurança. Os relatórios produzidos fornecem às partes interessadas a garantia de que o organismo é resiliente ciberneticamente e fornece provas de que os investimentos efetuados em cibersegurança geram os retornos esperados.

3. Boas práticas de Gestão da Cibersegurança

Existem vários modelos de operacionalização do processo de gestão da cibersegurança numa organização, dos quais se destacam o NIST Cybersecurity Framework e a norma ISO 27001. Em virtude do seu menor formalismo, e maior facilidade de implementação, recomenda-se a utilização do primeiro modelo no contexto autárquico, nada invalidando que, numa fase de desenvolvimento posterior, o OPL prossiga para a implementação da norma ISO 27001, a qual oferece a oportunidade da atribuição de uma certificação, caso tal se revele importante e necessário.

O quadro de trabalho de cibersegurança do NIST assenta na atuação em cinco vertentes, designadamente:

Vertente	Âmbito
1. Identificar	Que estruturas e práticas estão em vigor para identificar ameaças cibernéticas?
2. Proteger	Quais são as práticas básicas em vigor para proteger os seus sistemas?
3. Detetar	O que usa para identificar alguém ou algo malicioso?
4. Responder	Como vai lidar com uma violação se e quando ocorrer?
5. Recuperar	Como vai fazer o seu negócio voltar ao normal depois de uma violação?

I. Identificar

Porquê fazer isto?

Sem saber quem é o responsável pela cibersegurança, não pode começar a abordá-la. Além disso, sem saber que sistemas tem ou que software está a utilizar, não tem qualquer meio de compreender os controlos e itens de segurança que pode implementar, ou que podem já existir. Sem estas identificações, pode também não haver forma de identificar a potencial fonte de um evento de violação de segurança.

Quem é o responsável pela cibersegurança?

Este é o ponto de partida. Quem, no seu OPL, é responsável pela cibersegurança? Se está a ler este manual, é provável que seja o próprio, mas pode haver outra pessoa no seu organismo que assuma esta liderança.

Parceiros externos

Há alguém fora do seu organismo a quem possa recorrer para o ajudar com a cibersegurança ou para ajudar a definir e implementar proteções ou alterações aos seus sistemas de informação? Avalie do que efetivamente precisa e procure os parceiros certos para lhe prestar apoio.

Saber priorizar

À medida que trabalha nos próximos pontos e determina quais os dados, sistemas e software que mantém ou utiliza, tente priorizá-los em termos de criticidade. Do que precisa necessariamente para o seu organismo funcionar e o que é apenas um bom complemento? Este pensamento irá ajudá-lo a considerar quais os sistemas e aplicações que deve restaurar primeiro, em caso de desastre.

Que dados guarda?

Esta é a raiz de uma política de cibersegurança, por isso, aborde exaustivamente este ponto. Que dados mantém que podem ser úteis (ou rentáveis) para um cibercriminoso? Alguns exemplos incluem:

- Informações pessoais identificáveis (NIF, NISS, etc.);
- Informações do cartão de pagamento (Números de Cartões de Crédito);
- Informações de saúde pessoal;
- Registos de RH que podem conter informação sobre contas bancárias;
- Planos de negócios;
- Esquemas proprietários, pedidos de patente, etc.

Que dispositivos precisam de proteção?

Vamos pensar no que está a proteger do ponto de vista físico primeiro. Deve criar um inventário para os seus sistemas e dispositivos. Pense em tudo o que possa ser usado para aceder à informação do seu organismo: desktops e portáteis, obviamente, mas inclua smartphones e tablets aqui também. Pode dar-lhes uma designação simples, para conveniência do inventário (por exemplo, associando-o ao nome do respetivo utilizador).

Que sistemas operativos é que está a utilizar?

Certifique-se de que todos os seus sistemas operativos estão atualizados. Por exemplo, o suporte para o Microsoft Windows XP terminou a 8 de abril de 2014. Da mesma forma, a Apple terminou o suporte para OS X 10.6 em 26 de fevereiro de 2014. Estes sistemas podem ser vulneráveis a ataques e os seus fabricantes deixarão de os proteger. O seu OPL NÃO deveria estar a executar nenhum destes sistemas operativos. Certifique-se também de que os seus dispositivos móveis estão a funcionar atualmente com versões suportadas. Se não, é hora de atualizá-los. Um dispositivo com versões não suportadas é extremamente vulnerável a ataques.

Em que aplicações e serviços da nuvem está o organismo a guardar informação?

A informação é normalmente armazenada através de diferentes tipos de software, para pagamentos e dados de utentes, ou talvez num Software de Gestão de Relacionamento com o Cliente (CRM). Identifique os locais onde armazena os dados eletrónicos e documente, para cada um deles, quaisquer funcionalidades de segurança que necessite de utilizar para aceder aos dados, incluindo a especificação se pretende usar só uma palavra-passe ou uma autenticação baseada em dois fatores (onde introduz um número PIN após a sua senha). Além disso, inclua os serviços de armazenamento na nuvem.
Se conhecer a versão de um determinado software, documente-a também. Se não, procure perceber a versão logo que possível. Certifique-se de que a versão ainda está suportada pelo fabricante.

II. Proteger

O que pretendemos proteger?

Pretendemos proteger os itens que identificou na fase anterior. E, com isso, também a reputação do seu Organismo do Poder Local e os funcionários e utentes dos seus serviços.

Como proteger a informação da organismo?

Identificámos os dados que guarda no primeiro passo. Agora, vamos analisar as formas específicas de proteger esses dados. Ao longo do caminho, ofereceremos dicas e boas práticas de cibersegurança para proteger a sua informação e garantir que os seus colaboradores acedem a essa informação de forma segura. As melhores práticas podem e devem estender-se à sua vida privada também. Se não estiver a utilizar senhas complexas para as suas informações pessoais, aproveite para o fazer agora.

Como gere as contas dos utilizadores?

As contas dos utilizadores são um meio de determinar quem está a aceder aos dados e a que horas. Permitem também desativar um único utilizador nos seus sistemas, se necessário, em vez de ter de reautenticar todos os logins na sua rede ou sistemas.
Lembre-se que, se utilizar um sistema pessoal para iniciar sessão ou aceder aos dados do seu organismo, também deverá ter nomes de utilizadores separados para esse sistema. Os computadores privados com vários utilizadores podem ser mais suscetíveis a malware ou vírus do que máquinas de negócio dedicadas. Se utilizar um computador pessoal partilhado com outros membros da sua família, crie uma conta de utilizador em separado para fins profissionais e mantenha-a com um login e senha distintos.

Quão seguras são as suas palavras-passe?

A complexidade da palavra-passe é uma das peças mais fáceis do puzzle de cibersegurança para resolver. As melhores práticas incluem:

- **Complexidade:** um mínimo de três dos quatro seguintes: Letras maiúsculas, letras minúsculas, números, símbolos;
- **Comprimento:** Pelo menos oito caracteres;
- **Alterar frequência:** As palavras-passe são alteradas a cada 180 dias, pelo menos, mais se necessário por específico mandato (PCI-DSS, etc.);
- **Reutilização:** Não reutilizar as últimas seis palavras-passe;
- **Bloqueio:** bloqueio de 10 minutos após oito tentativas de login sem sucesso.

Contemple usar frases-passe

É recomendado o uso de frases-passe ao invés de palavras-passe, sempre que os sistemas do seu organismo suportarem a utilização de fra-

ses-passe. Estas são senhas muito longas que são facilmente memorizadas, mas extremamente difíceis para uma máquina adivinhar. Tornam o seu sistema mais seguro do que uma palavra-passe mais curta e podem ser mais fáceis de lembrar do que um amontoado de caracteres e símbolos (por exemplo: "O meu gato adora sair à noite!" Fácil de memorizar, não é?).

E as palavras-passe do dispositivo móvel?

Os dispositivos móveis que acedam à informação do OPL devem ser protegidos com, pelo menos, um número PIN de quatro dígitos. Se estiver a utilizar um leitor biométrico, como a sua impressão digital, recomendamos a utilização de uma palavra-passe mais complexa e segura, uma vez que não terá de a escrever com muita frequência.

Bloqueia os seus sistemas após um tempo de inatividade?

Os intervalos do sistema são uma boa forma de proteger os seus sistemas no caso de você ou um funcionário se afastar de um computador por um determinado período. Todos os computadores devem ser configurados para bloquear e exigir uma palavra-passe novamente após 5 minutos de inatividade.

Mais sobre as palavras-passe

Livros inteiros foram escritos sobre a criação e gestão de passwords. Embora as noções que recomendamos sejam atualmente o padrão da indústria, é necessário certificar-se de que a sua política de mudança de palavras-passe não está a criar vulnerabilidades.
Se você ou os seus colaboradores estiverem a ter tanta dificuldade em lembrar-se de senhas que têm de as escrever, enviar por e-mail ou armazená-las no telemóvel, terá de reavaliar e considerar a utilização de um gestor de passwords ou de outra forma de autenticação.
O nível de exigência associado à aplicação destes controlos de segu-

rança variará consoante o risco associado aos seus sistemas e serviços. Poderá utilizar o Ative Directory num ambiente Windows, ou recorrer a sistemas baseados na nuvem para controlar o ciclo de vida das palavras-chave. Se não tiver acesso a tais ferramentas, terá de investir mais na sensibilização dos colaboradores e recorrer a outros mecanismos para receber lembretes para a alteração de palavras-passe.

Encripta os seus dados?

A encriptação é algo que pode ser feito pela maioria dos OPL, independentemente do tamanho. No entanto, há coisas diferentes que podem ser encriptadas, e é importante entender o que são:

- **Bases de dados:** Bases de dados que contenham informações sensíveis, incluindo dados pessoais, informações pessoais de saúde e/ou dados de pagamento, devem ter alguma forma de encriptação no lugar. Isto não tem de ser toda a base de dados, visto que pode causar problemas de desempenho, mas as colunas dos dados que são considerados sensíveis (como números de segurança social) devem ser encriptados.

- **Discos rígidos do servidor:** Os discos rígidos do servidor podem ser encriptados se necessário. Isto vai garantir que a unidade é inacessível se for fisicamente removida ou roubada.

- **Discos rígidos de portáteis:** Os portáteis são suscetíveis a roubos ou perdas. Se tiver a capacidade de encriptar discos rígidos nesses sistemas, deve fazê-lo. Isto pode ser facilmente feito, sem grande investimento, com uma série de produtos diferentes. O BitLocker é um produto construído na tecnologia Microsoft que pode ser usada, e a Apple oferece também funcionalidades de encriptação.

- **Armazenamento em Dispositivos Móveis:** Os dispositivos móveis da Apple são automaticamente encriptados quando um PIN, número ou senha, é ativado. Os dispositivos Android requerem uma definição adicional para ativar a encriptação total.

- **E-mail em trânsito:** O e-mail pode ser encriptado em trânsito através da utilização de SSL/TLS, que é ativado por padrão na maioria dos servidores de correio. Só funcionará se o remetente e o destinatário tiverem a encriptação SSL/TLS ativada, por isso, é um processo baseado no melhor esforço aplicado. Esta encriptação só protegerá o e-mail de ser intercetado quando em trânsito.

Como se segregam dados?

Mesmo para os OPL de menor dimensão, colocar os dados em múltiplas pastas e restringir o acesso a cada uma delas apenas a quem precisa da informação, é uma boa prática. Para segregar adequadamente os dados, é necessário primeiro determinar quais os dados que recolhe e, em seguida, quem precisa de acesso a esses dados.
Pondere cuidadosamente ao longo deste processo, porque pode ser muito tentador dizer "todos precisam de tudo". Este é raramente o caso - especialmente com informações de RH, incluindo folhas de pagamento. Tome nota dos tipos de dados que poderá recolher e quem, no seu organismo, precisa de acesso aos mesmos. Quando voltar ao seu escritório, configure pastas e métodos de permissão para restringir o acesso a essas pastas.

Precisa de aceder remotamente aos ficheiros do seu organismo?

O acesso remoto aos sistemas de informação do OPL representa uma fonte de potenciais problemas. Por isso, deve garantir que, se a sua força de trabalho está em teletrabalho, os acessos a esses sistemas são adequadamente controlados. Os colaboradores que estão a trabalhar a partir de casa estão a usar senhas complexas? Quando é que foi a última vez que os sistemas operativos foram atualizados? O sistema antivírus está atualizado?
A formação neste ponto é também essencial. Se o seu OPL disponibiliza uma Rede Privada Virtual (VPN) para aceder a ficheiros no seu escritório, os colaboradores devem saber usar a VPN sempre que estiverem num

lugar público ou possam ter preocupações de segurança na ligação a partir do local onde se encontrem. Os colaboradores não devem ter acesso a qualquer informação sensível do organismo através de redes públicas, tais como as encontradas em cafés ou em aeroportos.

Como é que está a usar as firewalls?

As firewalls são dispositivos eficazes para bloquear atividades potencialmente maliciosas na sua rede e sistemas, pelo que o seu organismo deve ter, pelo menos, uma firewall instalada. Organismos com diferentes complexidades terão necessidades de firewall diferentes, pelo que, caso não se sinta preparado para optar pela melhor solução, deverá recorrer aos conselhos de um profissional especializado.

Como é que está a lidar com as atualizações dos seus sistemas?

As atualizações regulares do sistema operativo dos seus computadores pessoais e servidores de rede representa uma medida de segurança essencial. As fraquezas conhecidas são constantemente exploradas pelos hackers, por isso, certifique-se que os seus sistemas estão configurados para descarregar e aplicar os patches de sistema automaticamente e de forma frequente. Geralmente, é melhor deixar um sistema ligado durante a noite para aplicar patches quando não interfere com o seu trabalho.
Além dos sistemas operativos, aplicações como o seu navegador de internet, produtos da Adobe como o Acrobat Reader e Java, são atualizados com muita regularidade. Certifique-se de que está a incluir estes patches no seu ciclo de atualização regular, uma vez que são tão importantes como os patches do Sistema Operativo!

Como capacita os seus empregados?

Deve treinar regularmente os agentes e funcionários do seu OPL sobre as melhores práticas de cibersegurança, ou contrate um especialista com competências para o fazer. As formações devem ser ministradas

aquando da contratação de um novo colaborador e também anualmente, ou quando tal se revelar necessário.

Contemple usar autenticação de dois fatores?

A utilização de controlos de acesso e autorização baseados na autenticação de dois fatores representa um importante reforço dos mecanismos de segurança da sua organismo.
A autenticação de dois fatores está disponível através de aplicações comuns baseadas na nuvem, como Dropbox, Facebook, LinkedIn, Twitter e plataformas como o Microsoft 365 e o Google Apps. Este método consiste na utilização de dois mecanismos complementares de autenticação, que adicionam uma camada de segurança a qualquer processo de login, exigindo uma senha que é gerada aleatoriamente e enviada ao utilizador por mensagem de texto, e-mail ou via uma aplicação geradora de código, e é usada para além de uma senha normal.
Se utilizar dois fatores, mesmo que alguém obtenha a sua palavra-passe, geralmente não será capaz de iniciar sessão porque não será capaz de receber o número PIN secundário.

III. Detetar

O que estamos a detetar?

A deteção é o processo para reconhecer se está a ocorrer alguma tentativa de intrusão na sua rede e, se possível, impedi-lo.

Aplicações antivírus

Todos os sistemas necessitam de alguma forma de aplicação antivírus que seja instalada, atualizada e executada regularmente. As organizações de maior dimensão podem contemplar um programa unificado, que permite a um administrador fazer atualizações e exigir a digitalização a intervalos regulares.

Para organismos de menores dimensões, o Windows oferece software antivírus incorporado, e existem algumas opções gratuitas também. A coisa mais importante a lembrar quando estiver a instalar uma aplicação antivírus é que não fará nada por si só. Um programa antivírus precisa de ser programado para primeiro atualizar e, em seguida, em segundo lugar realmente executar para procurar vírus que podem ficar adormecidos ou não ser imediatamente aparentes.

Aplicações antimalware

As aplicações antimalware são semelhantes às aplicações antivírus, mas a maioria dos sistemas normalmente requer alguma combinação dos dois, uma vez que são projetados para abordar diferentes áreas. Semelhante às aplicações antivírus, existem muitos programas de antimalware, alguns gratuitos ou de baixo custo.
As ressalvas que se aplicam às aplicações antimalware também são válidas para as aplicações antivírus: Devem ser programadas para atualizações automáticas, bem como para executar diagnósticos regulares.
Além disso, esteja ciente de que, por vezes, as aplicações antimalware e antivírus podem entrar em conflito, pelo que deve estar atento a uma aplicação que pode identificar a outra como vírus ou malware potencial.

Soluções mais complexas de deteção

Existem soluções mais complexas de deteção que uma organização maior, ou com informações particularmente sensíveis, poderá querer usar para reforçar ainda mais a segurança das suas redes. Essas soluções incluem firewalls de última geração que oferecem uma gestão unificada de ameaças, incorporando as funções de uma firewall tradicional (portas de bloqueio, etc.) mas também a filtragem web e de e-mails. Estes dispositivos podem fornecer relatórios e outros resultados que permitam notificar os responsáveis de uma organização quando esta estiver sob algum tipo de ataque. Estas soluções são normalmente personalizadas para cada negócio e requerem algum conhecimento para configurar corretamente. Em caso de dúvida, recomendamos procurar um profissional de TI para ajudá-lo.

Determinar o Impacto de um Evento

Quando descobrir um evento (por exemplo, malware no seu sistema), terá de fazer uma determinação do impacto desse evento. Geralmente, o seu programa antivírus ou programa antimalware bloqueará a maioria das tentativas de instalação de vírus ou malware. Neste caso, o impacto é bastante baixo - o programa bloqueou-o e segue em frente com o seu dia.
No caso de um código malicioso chegar aos seus sistemas, terá de determinar qual é o propósito desse código (por exemplo, é ransomware à procura de um pagamento ou um leitor de teclas projetado para roubar nomes de utilizadores e palavras-passe?)
Com esse entendimento pode determinar o impacto que a peça de malware ou vírus tem no seu negócio e começar a tomar medidas para responder.

IV. Responder

Como reagimos a um incidente?

Em primeiro lugar, precisa de ter um plano preparado para responder a incidentes. A resposta e recuperação de incidentes de segurança de TI é uma área com a qual os organismos do Poder Local podem ter algumas dificuldades. Os OPL de menores dimensões geralmente não têm tempo para criar planos elaborados e para testá-los, por isso, é preciso planear de uma forma que funcione para o seu organismo. Se possuir dados dos seus utentes e tiver desenvolvido algumas diligências neste processo através de uma declaração de privacidade, então deverá levá-la a sério. Se a seu organismo é de pequenas dimensões e evitou agregar informações sensíveis, ainda assim deve demorar algum tempo para entender estes conceitos e ter uma ideia básica de como responder à intrusão de forma a proteger o seu negócio.

Com que frequência faz backups?

Uma das formas de ataque mais prevalentes hoje é a variante criptolocker de malware. Quando este tipo de malware é instalado num sistema, todos os fichei-

ros estão bloqueados e é pedido um resgate para obter a chave para desbloqueá-los. O seu único recurso neste evento é recorrer aos seus backups. Mas tem que prever backups para os ter disponíveis quando forem necessários.

Quando define um esquema de backup (isto é, quantas vezes faz backup de sistemas e o que inclui na operação de backup) precisa de determinar a quantidade de informação (do ponto de vista do tempo) que está disposto a perder. O backup demora uma hora? Um dia? Uma semana? Tome esta decisão em tempo útil e crie uma infraestrutura de backup para os seus sistemas que satisfaça estes requisitos, bem como a quantidade de informação (contabilizada em tempo) que o seu organismo poderá perder sem produzir um impacto relevante na sua atividade.

Precisa de analistas forenses digitais?

Os analistas forenses digitais podem ser necessários em caso de intrusão, a fim de determinar que informações foram realmente furtadas. Este conjunto de competências é muito especializado e a maioria dos organismos do Poder Local não possui as capacidades internas necessárias para executá-las. Recomendamos que encontre uma empresa ou um profissional que possa prestar estes serviços. Não precisa necessariamente tê-los contratados de antemão, mas saber a quem poderá ligar e talvez ter uma conversa inicial sobre como preservar ficheiros para trabalho forense vai ajudá-lo.

Circunscrever o impacto de um evento

Na medida do possível, quando descobrir um evento de cibersegurança, vai querer contê-lo. Os sistemas que tenham sido infetados com malware ou um vírus devem ser removidos da rede o mais rapidamente possível. Não desligue um sistema, pois pode perder provas forenses valiosas.

Incorporando Lições Aprendidas

À medida que reage a um evento, vai querer sempre incorporar as lições que aprendeu no seu programa interno de cibersegurança. A ideia é que quererá evitar que o mesmo tipo de ataque volte a acontecer. Se foi alvo de

um ataque de criptolocker, aproveite para treinar os seus colaboradores e a si mesmo na identificação de ligações maliciosas. Se perdeu dados que não eram recuperáveis porque o seu esquema de backup não o abordou adequadamente, aproveite para voltar e corrigir aquela área novamente. Ninguém é 100% impermeável a ciberataques, mas uma fraqueza real seria ter o mesmo tipo de ataque a afetar o seu organismo várias vezes sem tomar medidas para identificar as causas principais. Crie uma tabela para ajudá-lo a identificar as lições retiradas de eventos de intrusão que tenham ocorrido, registando na mesma a seguinte informacão:

- Data do incidente;
- Descrição do incidente;
- Como é que o incidente foi detetado?
- Como é que a situação foi contida?
- Dados afetados;
- Ações realizadas para eliminar a vulnerabilidade explorada.

V. Recuperar

O que é a recuperação?

A recuperação consiste em levar a atividade do organismo de volta a um estado pré-incidente o mais rápido e suavemente possível.

Voltar a juntar as peças

As noções de resposta e recuperação andam de mãos dadas, mas deve fazer de tudo para salvaguardar a continuidade da atividade da sua organismo e proteger os seus utentes em caso de incidente significativo. Mais uma vez, o tempo, os recursos e as despesas devem ser tidos em consideração, mas convém pensar "no dia seguinte". A quem vai ligar primeiro? Como garante que as suas ações ajudarão o seu organismo a evitar danos à sua reputação?

Quem são os seus recursos?

Antes de ocorrer uma intrusão, identifique quais os recursos necessários para ajudá-lo em caso de um evento sério de segurança de TI ou incidente que envolva os dados confidenciais dos seus utentes. Em caso de violação, a sua primeira chamada deve ser provavelmente para um especialista que o ajude a conter os efeitos do ataque, e a segunda para obter apoio jurídico, designadamente um advogado com conhecimento especializado na matéria, caso se venha a justificar-se alguma ação legal.

Reportar um incidente

A complexidade e a transnacionalidade de uma boa parte dos incidentes de cibersegurança requerem uma visão agregada e a ação coordenada entre as várias entidades envolvidas. Neste sentido, o Centro Nacional de Cibersegurança (CNCS) presta um serviço de coordenação na resposta a incidentes, que inclui:

- A triagem de notificações de incidentes, a sua análise técnica e forense;
- A articulação com as entidades nacionais e internacionais envolvidas;
- A produção de recomendações de mitigação e/ou de resolução do incidente;
- A coordenação da resposta a incidentes pode partir da iniciativa do CNCS, por exemplo numa situação de incidente de larga escala, ou ser-lhe solicitada pelos canais designados para o efeito. Em caso de necessidade ou de força maior, o CNCS coordena as suas ações com as restantes autoridades nacionais.

Para solicitar o serviço, deverá reportar o seu incidente através de um dos seguintes meios:

- Formulário disponível na página do CNCS para Notificação de Incidentes;
- Mensagem de correio eletrónico para cert@cert.pt, contendo informação detalhada sobre o mesmo;
- Em caso de urgência, poderá utilizar o contacto telefónico 210 497 399.

4. Gestão de utilizadores

O objetivo consiste em garantir o acesso autorizado dos utilizadores e impedir o acesso não autorizado aos sistemas de informação.

I. Criação e cancelamento de contas de utilizadores

Todas as ações de acesso devem ser rastreáveis a um indivíduo ou processo identificável. Deve haver um processo formal de registo e eliminação de contas de funcionários para a concessão de acesso a todos os sistemas de informação.

Registo dos utilizadores

O registo dos utilizadores deve ser gerido de acordo com as seguintes práticas:

- Garantir que os pedidos de acesso são previamente aprovados pelo responsável competente;
- Assegurar que as razões para solicitar o acesso são coerentes com as responsabilidades da função a desempenhar;
- Manter registos das aprovações de direitos de acesso;
- Garantir que os funcionários compreendem as condições de acesso e, quando adequado, assinam acordos de confidencialidade;
- Garantir que os acessos são rastreáveis a um indivíduo ou processo identificável;
- Certificar que é criada uma conta individual para cada colaborador poder aceder aos sistemas de informação.

Cancelamento de contas de acesso

O cancelamento de contas dos utilizadores deve ser assegurado de acordo com as seguintes práticas:

- Remover os privilégios de acesso aos funcionários que já não estão na organização no prazo de 5 dias úteis;
- Rever prontamente os direitos de acesso sempre que um funcionário mude de deveres e responsabilidades;
- Rever prontamente os direitos de acesso sempre que o departamento do funcionário estiver envolvido numa reorganização significativa;
- Rever os privilégios de acesso dos funcionários em falta prolongada ou cessão temporária no prazo de 10 dias úteis a contar da mudança de estatuto;
- Remover os privilégios de acesso a qualquer funcionário dispensado por justa causa com o envio da respetiva notificação;
- Verificar trimestralmente para remoção de contas de utilizador inativas ou redundantes.

Autoridade e Exceções

Os funcionários individuais podem ter várias contas quando:

- Necessário para satisfazer limitações de tecnologia;
- Esteja obrigado a satisfazer requisitos de negócio únicos desde que a fundamentação fique documentada e seja aprovada pelo responsável competente.

II. Fornecimento de acesso ao utilizador

A finalidade é garantir o acesso autorizado do utilizador e impedir o acesso não autorizado do utilizador a sistemas e serviços. Um identificador (ID) de login único e senha é atribuído a todos os utilizadores, com privilégios variados, dependendo das funções e requisitos. A identificação e autenticação do utilizador é implementada de acordo com os privilégios

concedidos ao respetivo utilizador. Deve ser implementado um processo formal de fornecimento de acesso aos funcionários para atribuir ou revogar direitos de acesso de todos os tipos de utilizadores a todos os sistemas e serviços. Os proprietários de informações e os guardiões da informação devem implementar um processo formal de fornecimento de acesso aos funcionários. O processo de provisionamento para a atribuição ou revogação dos direitos de acesso concedidos aos IDs dos utilizadores deve incluir:

- Obtenção de autorização do proprietário do sistema de informação ou serviço para a utilização do sistema de informação ou serviço. Pode igualmente ser adequada a aprovação separada dos direitos de acesso para gestão;
- Verificar se o nível de acesso concedido é adequado às políticas de acesso e é coerente com outros requisitos, tais como a segregação de direitos;
- Garantir que os direitos de acesso não são ativados (por exemplo, por prestadores de serviços) antes de os procedimentos de autorização serem concluídos;
- Manter um registo central dos direitos de acesso concedidos a um ID do utilizador para aceder a sistemas e serviços de informação;
- Adaptação dos direitos de acesso dos funcionários que tenham mudado de funções e remover imediatamente ou bloquear imediatamente os direitos de acesso dos funcionários que deixaram o organismo;
- Rever periodicamente os direitos de acesso com os proprietários dos sistemas ou serviços de informação.

III. Gestão das senhas dos utilizadores

O objetivo é definir os processos formais de gestão para a emissão de senhas. A emissão e revogação das credenciais de autenticação devem ser controladas através de um processo formal de gestão. O OPL deve designar formalmente indivíduos que tenham autoridade para emitir e redefinir palavras-passe, aplicando-se o seguinte:

- As palavras-passe só devem ser emitidas aos funcionários cuja identidade seja confirmada antes da emissão;

- Os indivíduos com autoridade para repor palavras-passe devem transmitir senhas novas ou repostas ao funcionário de forma segura (por exemplo, utilizando encriptação, utilizando um canal secundário);
- Sempre que tecnicamente possível, as palavras-passe temporárias devem ser únicas para cada indivíduo e não devem ser facilmente calculadas;
- As palavras-passe nunca devem ser armazenadas de forma desprotegida;
- As palavras-passe predefinidas fornecidas pelos fornecedores de tecnologia devem ser alteradas para uma palavra-passe conforme com as normas durante a instalação da tecnologia (hardware ou software);
- A revogação das credenciais de autenticação deve seguir um processo formal.

IV. Revisão dos direitos de acesso do utilizador

O objetivo é garantir que os direitos de acesso só existam para os utilizadores com uma "necessidade de saber" definida. Os privilégios dos utilizadores do organismo serão revistos regularmente. O Administrador do Sistema reverá os direitos de acesso e o respetivo responsável de área ratificará o relatório de revisão. Os proprietários de informação devem rever formalmente os direitos de acesso dos funcionários a intervalos regulares.

Circunstâncias e critérios para revisão formal do direito de acesso

Os proprietários devem implementar processos formais para a revisão regular dos direitos de acesso. Os direitos de acesso devem ser revistos:

- Anualmente;
- Mais frequentemente para ativos de informação de alto valor e utilizadores privilegiados;
- Quando a situação de um funcionário muda como resultado de uma promoção, despromoção, remoção de um grupo de utilizador, reafectação, transferência ou outra alteração que possa afetar a neces-

sidade de acesso de um colaborador aos ativos de informação;
- Como parte de uma grande reorganização, ou a introdução de novas tecnologias ou aplicações;
- Quando os Proprietários de Informação mudam a política de controlo de acesso.

Procedimento para revisão formal dos direitos de acesso

A revisão dos direitos de acesso deve incluir:

- Confirmação de que os direitos de acesso se baseiam nos princípios necessários e na regra do menor privilégio necessário;
- Confirmação de que o utilizador tem efetiva necessidade de acesso;
- Revisões e verificação das listas de controlo de acessos datadas e assinadas pelo revisor e mantidas para efeitos de auditoria;
- Confirmação de que as alterações aos direitos de acesso são registadas e auditáveis.

Os registos e relatórios de controlo de acesso são registos da organização e devem ser mantidos e eliminados de acordo com o calendário aprovado de gestão de registos.

V. Remoção ou alteração dos direitos de acesso

O objetivo é garantir que os direitos de acesso físico e lógico aos sistemas de informação e às instalações de processamento de informação sejam geridos em relação às responsabilidades de segurança dos requisitos de trabalho. Os direitos de acesso de todos os funcionários, fornecedores e utilizadores de terceiros às instalações de informação e tratamento de informação são removidos após a cessação do seu contrato, ou ajustados após a sua alteração. Os direitos de acesso dos funcionários aos sistemas de informação devem ser suprimidos após a cessação da relação laboral e revistos após a alteração do estatuto laboral.

Alteração do estatuto laboral

Os responsáveis de área devem rever o acesso aos sistemas de informação e às instalações de processamento de informação quando ocorrer alteração da relação laboral, incluindo:

- Quando os funcionários assumem novas funções e responsabilidades;
- Durante a reestruturação de funções e responsabilidades posicionais ou organizacionais;
- Quando os funcionários iniciam uma licença de longa duração;
- Atualizar diretórios, documentação e sistemas.

Ação após cessação ou alteração do emprego

Os responsáveis de área devem assegurar que o acesso aos sistemas de informação e às instalações de tratamento de informação seja removido após a cessação da relação laboral ou revisto após a mudança de emprego:

- Remover ou modificar o acesso físico e lógico;
- Recuperação ou revogação de dispositivos de acesso, cartões e chaves;
- Atualizar diretórios, documentação e sistemas.

5. Responsabilidades e deveres do utilizador

I. Obrigações gerais e uso da Internet

Sugere-se a adoção das seguintes regras de uso da Internet no organismo de Poder Local:

Os funcionários e fornecedores não utilizarão, em caso algum, os meios informáticos e sistemas de informação do organismo, para:

1. Exercer qualquer atividade ilegal ou violar os direitos de qualquer indivíduo;
2. Descarregar ou instalar software de qualquer tipo sem autorização;
3. Copiar ou distribuir qualquer material protegido por direitos autorais sem autorização;
4. Aceder às informações pessoais de outras pessoas sem autorização, exceto no âmbito das funções que lhe tiverem sido atribuídas;
5. Fazer quaisquer reclamações ou marcação de uma posição, em nome do organismo, a entidades terceiras, a menos que tenha autorização para fazê-lo;
6. Desenvolver qualquer atividade que prejudique a reputação da organismo;
7. Visitar sítios web que exibam material sexualmente explícito ou imoral, sites de jogo ou outros sites relacionados com atividades ilegais;
8. Visitar sítios web que incentivem a violência, discriminação ou violação dos direitos de qualquer grupo ou indivíduo, exceto no decurso de pesquisas autorizadas;
9. Visitar sítios web que partilhem música ou outros ficheiros numa base *peer-to-peer* ou partilhem conteúdo em violação da legislação de direitos autorais;
10. Exercer qualquer atividade ilícita que prejudique as plataformas di-

gitais e computacionais do organismo, bem como a capacidade de outra organização ou indivíduo para realizar atividades de computação (por exemplo, através de ataques de negação de serviço);

11. Fornecer quaisquer informações sobre o organismo ou respeitantes aos seus funcionários, fornecedores e utentes dos serviços públicos que presta, a qualquer entidade externa, a menos que explicitamente autorizado a fazê-lo;
12. Publicar comentários ou outras informações em sites de redes sociais ou blogs em nome do organismo ou usando endereços de e-mail do organismo, a menos que explicitamente autorizado a fazê-lo.

II. Partilha de Ficheiros Online, Backup e Sincronização

Os serviços de partilha de ficheiros online, backup e sincronização, tais como Dropbox, Google Drive, OneDrive, etc. são formas muito convenientes de armazenar e partilhar ficheiros online, mas aumentam o risco de que informações confidenciais ou informações protegidas sejam indevidamente partilhadas.
Assim, com vista a mitigar esses riscos, quaisquer informações ou dados relacionados com a atividade do organismo não podem ser copiadas ou armazenadas em nenhum sistema de partilha de ficheiros online ou de backup sem autorização específica do organismo, exceto aqueles que já tenham sido oficialmente instalados e configurados pelos departamentos competentes, no seu posto de trabalho.

III. Transmissão de informações protegidas

Os funcionários e fornecedores não devem transmitir nenhuma Informação Protegida, ou declarada como confidencial, em qualquer e-mail ou através de qualquer serviço de mensagens ou chat instantâneos, devendo informações deste tipo ser transmitidas através de um método de transferência de ficheiros seguro.

IV. Locais de armazenamento autorizados

Todas as Informações Protegidas serão processadas e armazenadas com recurso às aplicações e serviços autorizados pelo organismo. Nenhum funcionário ou fornecedor pode copiar qualquer Informação Protegida para qualquer outro local, a menos que seja direcionado para tal por um responsável autorizado do organismo.

V. Uso do correio eletrónico (e-mail)

O e-mail é uma importante ferramenta de comunicação, mas também tem o potencial de causar danos a qualquer organização. O uso inadequado de e-mails pode resultar na perda de dados sensíveis ou confidenciais da organismo, assim como danos à imagem pública ou em sistemas internos críticos e exposição não intencional dos funcionários a conteúdos ou materiais inadequados. Frequentemente, se usado de forma desatenta, pode também ser usado como porta de entrada para ataques de elevado impacto, como é o caso do *ransomware*.

Assim, os trabalhadores e fornecedores não devem participar em nenhuma das seguintes atividades:

1. Enviar mensagens de correio eletrónico não solicitadas, incluindo "correio publicitário" ou outro material publicitário a indivíduos que não solicitaram especificamente esse material (correio publicitário não solicitado);
2. Assediar sob qualquer forma, seja através da linguagem, frequência ou tamanho das mensagens;
3. Criar ou reencaminhar "correntes", cadeias "Ponzi" ou esquemas de "pirâmide" de qualquer tipo;
4. Enviar mensagens de correio eletrónico semelhantes a partir de vários endereços de e-mail com a intenção de assediar ou obter respostas;
5. Forjar cabeçalhos de e-mail.

VI. Descarregar ou instalar software

Os funcionários e fornecedores não devem poder descarregar ou instalar qualquer aplicação de software sem a autorização de um representante autorizado do organismo, podendo ser configuradas políticas ao nível do sistema operativo Windows que impeçam essas ações sem a detenção de privilégios de administrador.

VII. Acesso remoto e redes sem fios pessoais

Nenhum funcionário ou fornecedor deverá poder instalar qualquer dispositivo de rede sem fios que se conecte às redes do organismo, nem qualquer software ou aplicação que permita o acesso aos sistemas da organização a partir de um local remoto sem a autorização do responsável competente.

6. Boas práticas na Ótica do utilizador

Embora a utilização dos meios digitais, quer sejam computadores ou serviços online, se tenha tornado parte familiar e comum do nosso trabalho e da nossa vida quotidiana, a Internet oferece muitos perigos para os quais importa estarmos preparados. Com efeito, as informações que publicar online e os registos de sites que visitou podem ser utilizados para publicidade direcionada, mas também para fraudes direcionadas, através das quais os vigaristas tentam enganá-lo para que lhes dê informações que em seguida utilizarão para roubá-lo. Saiba, desde já, que se o seu computador estiver ligado à Internet, estará sob ataque constante, não só por hackers que o fazem por mero desporto, mas também por organizações criminosas que procuram explorar recursos informáticos para roubar informações, enviar e-mails de spam, distribuir material ilícito ou atacar outros computadores.
Assim, dado que os cibercriminosos prosperam com más práticas de segurança dos utilizadores e das organizações, a nossa melhor defesa consiste em construirmos bons hábitos de segurança e encorajarmos todos os que conhecemos a fazer o mesmo.

I. Mantenha a sua mesa limpa

Faz todo o sentido e soa tão simples, mas manter uma mesa limpa é muitas vezes negligenciado quando se fala de segurança de dados. É também o lugar perfeito para começar a abordar o tema da cibersegurança com os colegas.
Os funcionários que mantêm uma secretária desordenada tendem a deixar as unidades USB e os smartphones à vista. Também, muitas vezes, esquecem-se de proteger fisicamente os computadores portáteis para evitar para evitar que alguém saia discretamente com eles.
Uma mesa desarrumada também torna mais difícil perceber que algo está a

faltar, como uma pasta com cópia impressa em papel de informações confidenciais. Além de aumentar a probabilidade de algo ser retirado, uma mesa desordenada significa que a descoberta de qualquer roubo provavelmente será adiada, provavelmente por dias, ou até mesmo semanas, se o funcionário estiver fora do escritório. Estes atrasos dificultam a determinação de quem é o prevaricador e onde o material roubado pode estar agora localizado.
Encorajar os funcionários a manter uma mesa limpa compensa de duas formas. De facto, para além de tornarem os ativos digitais e de papel mais seguros, os funcionários com mesas limpas são mais aptos a serem produtivos porque podem aceder rapidamente e de forma segura às ferramentas e recursos de que necessitam para fazerem o seu trabalho.

II. Bloqueie automaticamente a sua sessão no computador

Deve bloquear o ecrã sempre que se ausentar do seu computador, o que pode rapidamente fazer através da combinação de teclas Ctrl+Alt+Delete/Bloquear. Pode também ativar um protetor de ecrã que, em caso de inatividade, desligue a imagem após um minuto de inatividade e bloqueie automaticamente o ecrã após 5 minutos, exigindo uma palavra-passe/frase-passe para desbloqueá-lo. Isto é necessário, porque uma pessoa não autorizada pode ver informações sensíveis, manipular o seu e-mail ou sites de redes sociais, ou explorar o acesso ao seu computador de outras formas.
Para a sua própria proteção, no final do dia de trabalho, termine sempre a sessão do ambiente de trabalho do seu computador.

III. Práticas de cibersegurança em teletrabalho

Se estiver a trabalhar a partir de casa, tem de assegurar que a sua rede doméstica sem fios está devidamente configurada e protegida. Aprenda a protegê-la, conforme indicado abaixo.

Não se esqueça dos documentos em papel! As informações impressas ainda representam um risco de segurança se não forem devidamente armazenadas e eliminadas, pelo que deve adotar as seguintes práticas de prevenção:

1. Não dê folhas de papel antigas, impressas de um lado com conteúdos do organismo ou de outras entidades, para os seus filhos fazerem desenhos no outro, pois podem ser inadvertidamente levados para fora de casa (por exemplo, para a escola ou outros lugares) e nunca se sabe quem poderá vir a lê-los;
2. Tenha igualmente cuidado com os documentos de trabalho inúteis que são colocados nos locais públicos de reciclagem, devendo ser previamente destruídos;
3. Procure utilizar um triturador transversal para inutilizar os documentos sensíveis.

Ter uma rede doméstica aberta ou insuficientemente protegida é um alto risco, pois pode permitir que intrusos vejam a sua atividade, recolham informações sobre si ou utilizem a sua rede para fins nefastos. Estes podem levar a potenciais problemas legais, falhas de serviço, problemas de desempenho na rede, invasões de privacidade e roubo de identidade.
Com vista a tornar a sua rede doméstica mais segura, para além de dever consultar a documentação do fabricante, que veio com o seu router sem fios, para seguir as configurações recomendadas, considere implementar as sugestões abaixo:

1. **Altere a palavra-passe predefinida do administrador.** A senha padrão que veio com o seu router é a mesma senha usada em milhões de outros routers da mesma marca e modelo. É a primeira senha que será tentada por um intruso;

2. **Desative o Plug-n-Play Universal (uPnP).** O UPnP é uma ferramenta incorporada nos routers que adiciona automaticamente dispositivos suportados à sua rede. Muitas versões de uPnP usadas em routers também são vulneráveis. A opção mais segura é desligá-la;
3. **Desative o acesso remoto.** Tal como os computadores, existem vulnerabilidades em muitos routers que podem permitir que alguém descubra a sua senha de administrador ou obtenha acesso não apro-

vado à sua rede. Um perigo particular é a capacidade de uma pessoa maliciosa aceder ao utilitário de configuração do router sem fios, fornecendo assim um caminho para tentar outras formas de explorações. Ao desativar a funcionalidade de acesso remoto, apenas um computador ligado diretamente ao router, através de um cabo de rede, terá acesso ao menu de configuração;

4. **Atualize o firmware regularmente.** O firmware é o software que o router executa para funcionar. Muitas vezes, os fabricantes oferecem novas versões de firmware que corrigem problemas de segurança e desempenho. Todavia, mesmo que o equipamento pertença a um operador, não assuma como dado garantido que essas atualizações sejam efetuadas automaticamente;

5. **Utilize encriptação WPA2 (AES) ou WPA3.** A encriptação WPA3 é atualmente a encriptação mais segura oferecida com routers domésticos e pode ser selecionada como uma opção ao ligar dispositivos à sua rede. Se não for suportado, utilize o WPA2 (AES) em vez disso. Isto não só impedirá alguém de intercetar as suas comunicações sem fios, como ajuda a proteger a sua rede de dispositivos de estranhos;

6. **Altere o SSID predefinido.** O SSID (Identificador de Conjunto de Serviços, ou *Service Set Identifier*) é o nome de rede sem fios que o router anuncia para o resto dos dispositivos na rede local. Normalmente, o SSID predefinido exibe informações do fabricante e do modelo. Altere o SSID para algo que não forneça informações sobre dispositivos, uma vez que estas informações podem ser utilizadas para tentar atacar o seu equipamento;

7. **Garanta a ativação da firewall incorporada no router.** Uma firewall é uma coleção de configurações no router que determina qual é o tráfego de dados que pode entrar na sua rede e que tráfego deve rejeitar. A firewall ajuda a proteger todos os dispositivos da sua rede, pelo que é do seu interesse saber mais sobre o uso de firewalls. Os routers mais antigos não têm firewalls incorporadas, por isso, verifique a documentação do fabricante do router e substitua-o, se for o caso;

8. **Certifique-se de que todos os dispositivos da sua rede doméstica foram configurados com a segurança em mente.** Utilize senhas de administrador complexas e dispositivos renomeados na sua rede para que o fabricante e o modelo do dispositivo não possam ser recolhidos visualizando o nome da rede do dispositivo. Lembre-se de verificar todos os seus dispositivos da sua rede, nomeadamente, computadores, impressoras, câmaras web, smartphones, tablets, etc. Não se esqueça que muitos eletrodomésticos já possuem funcionalidades de comunicação por Wi-Fi, pelo que não podem ser ignorados do ponto de vista da segurança, uma vez que, se incorretamente configurados, podem constituir potenciais portas de entrada na sua rede doméstica. Consulte os respetivos manuais de utilizador para saber como deve proceder;

9. **Utilize a lista de autorizações do Endereço MAC.** Um endereço MAC é o número único atribuído a todos os dispositivos que têm a capacidade de se ligar à rede. Alguns dispositivos têm mais de um endereço MAC devido a várias opções de conectividade de rede disponíveis (com fios, sem fios, Bluetooth). Assim, pode configurar o seu router apenas para permitir dispositivos com o endereço MAC associado aos seus dispositivos, o que ajuda a evitar que dispositivos não intencionais se conectem ao seu router;

10. **Configure uma rede Wi-Fi separada para os seus convidados.** Ativando esta configuração no seu router, uma parte da sua rede será utilizada para todos os seus dispositivos pessoais e domésticos, isolada da primeira, será utilizada para os hóspedes poderem ligar os seus dispositivos. Esta ação permite um acesso fácil à internet para os hóspedes, enquanto protege a sua rede pessoal e os seus dispositivos. Isto pode ser crítico se algum dos dispositivos dos seus hóspedes estiver comprometido com vírus que tentará infetar outros dispositivos na mesma rede.

IV. Proteja-se contra os ataques de engenharia social

6.IV.1 O que é a engenharia social?

A engenharia social é o termo usado para uma ampla gama de atividades maliciosas realizadas através de interações humanas. Usa manipulação psicológica para enganar os utilizadores e levá-los a cometerem erros de segurança ou a darem informações sensíveis.
O que torna a engenharia social especialmente perigosa, é o facto de se basear em erros humanos, em vez de vulnerabilidades em software e sistemas operativos. Os erros cometidos por utilizadores legítimos são muito menos previsíveis, tornando-os mais difíceis de identificar e frustrar do que uma intrusão baseada em malware.

6.IV.2 Técnicas de ataque de engenharia social

Os ataques de engenharia social podem surgir de formas diferentes e ser realizados em qualquer contexto em que a interação humana esteja envolvida. As cinco formas mais comuns de assaltos à engenharia social digital são descritas abaixo.

Baiting (isco)

Como o nome indica, os ataques de Baiting usam uma falsa promessa (isto é, um isco) para despertar a ganância ou curiosidade da vítima. Eles atraem os utilizadores para uma armadilha que rouba as suas informações pessoais ou infeta os seus sistemas com malware.
A forma mais difundida de Baiting usa meios físicos para difundir malware. Por exemplo, os atacantes deixam o isco - normalmente unidades de flash infetadas por malware - em locais visíveis onde as potenciais vítimas certamente as encontrem (por exemplo, casas de banho, elevadores ou o estacionamento da instituição alvo). O isco tem um aspeto

autêntico, com um rótulo que o apresenta como, por exemplo, a folha de pagamentos da organização. Então, as vítimas apanham o isco por curiosidade e inserem-no num computador de trabalho ou de casa, resultando numa instalação automática de malware no seu sistema.
Os esquemas de Baiting não têm necessariamente de ser realizados com base no mundo físico. As formas online de isco consistem em anúncios apelativos que levam para sites maliciosos ou que incentivam os utilizadores a descarregar uma aplicação infetada por malware.

Scareware (medo)

A técnica de Scareware consiste no bombardeamento das vítimas com falsos alarmes e ameaças fictícias. Os utilizadores são enganados e levados a pensar que o seu sistema está infetado com malware, induzindo-os a instalar software que não tem nenhum benefício real ou é, ele próprio, o malware. O Scareware também é referido como software de engano, software de scanner fraudulento e software fraudulento (fraudware).
Um exemplo comum de Scareware são os banners popup de aparência legítima que aparecem no seu browser enquanto navega na web, exibindo textos como: "O seu computador pode estar infetado com programas de spyware prejudiciais." A mensagem propõe-se a instalar uma ferramenta que supostamente o ajudará a limpar o seu computador, mas que é, muitas vezes, o próprio software malicioso, ou alternativamente irá direcioná-lo para um site malicioso onde o seu computador fica infetado.
O Scareware também é disseminado através de e-mail de spam, distribuindo avisos falsos ou fazendo ofertas para os utilizadores comprarem serviços inúteis ou nocivos.

Pretexting (pretexto)

Através desta técnica, o agressor obtém informações mediante uma série de mentiras habilmente trabalhadas. O esquema é frequentemente iniciado por alguém que finge precisar de informações sensíveis da vítima, com base no pretexto de que precisa realizar uma tarefa crítica.
O agressor começa geralmente por estabelecer confiança com a vítima,

fazendo-se passar por colegas de trabalho, polícias, funcionários bancários e fiscais, ou outras pessoas com algum tipo de autoridade. O agressor faz perguntas que são ostensivamente necessárias para confirmar a identidade da vítima, através das quais recolhem dados pessoais importantes. Todos os tipos de informações e registos pertinentes são recolhidos usando este esquema, tais como números de segurança social, endereços pessoais e números de telefone, registos telefónicos, datas de férias do pessoal, dados bancários e até informações de segurança relacionadas com uma instalação física.

Phishing

O Phishing é um dos tipos de ataques de engenharia social mais populares, sendo efetuados através de esquemas baseados em campanhas de e-mail e mensagens de SMS, destinadas a criar uma sensação de urgência, curiosidade ou medo nas vítimas. Em seguida, coloca-os a revelar informações confidenciais, depois de clicarem em links para sites maliciosos ou abrirem anexos que contenham malware.
Um exemplo típico é um e-mail enviado aos utilizadores de um serviço online que os alerta para a existência de uma violação das políticas instituídas e que, para a regularização da situação, requer uma ação imediata da sua parte, como seja uma alteração de senha de acesso. O ataque inclui um link para um website ilegítimo – quase idêntico à sua versão legítima – levando o utilizador insuspeito a introduzir as suas credenciais atuais e a nova senha. Após o formulário de submissão, a informação é enviada ao agressor.
Dado que mensagens idênticas, ou quase idênticas, são enviadas a todos os utilizadores em campanhas de phishing, detetá-las e bloqueá-las torna-se mais fácil para aqueles servidores de correio que dispõem de acesso a plataformas de partilha de informações sobre ameaças.

Spear Phishing

Esta é uma versão mais direcionada do esquema de phishing em que um intruso escolhe indivíduos ou organizações específicas. Em seguida, adaptam as suas mensagens com base em características, posições de empre-

go e contatos pertencentes às suas vítimas para tornar o seu ataque menos suspeito. O Spear Phishing (ou phishing de lança, em português) requer muito mais esforço da parte do agressor e pode levar semanas ou meses para conseguir alcançar os seus objetivos. São muito mais difíceis de detetar e têm melhores taxas de sucesso se forem feitos com habilidade.
Um cenário de Spear Phishing pode envolver um intruso que, ao fazer-se passar por consultor de TI de uma organização, envia um e-mail a um ou mais funcionários. É redigido e assinado exatamente como o consultor normalmente o faria, levando os destinatários a pensarem que é uma mensagem autêntica. A mensagem induz os destinatários a alterarem a sua palavra-passe através de um link que os encaminha para uma página maliciosa, onde o intruso captura as suas credenciais.

6.IV.3 Como deve prevenir-se dos ataques de engenharia social

Os engenheiros sociais manipulam sentimentos humanos, como a curiosidade ou o medo, para realizar esquemas e atrair as vítimas para as suas armadilhas, pelo que deve desconfiar sempre que se sentir alarmado com um e-mail ou atraído por uma oferta irrecusável num determinado site.

Estar alerta poderá ajudar a proteger-se da maioria dos ataques de engenharia social que ocorrem no domínio digital. As seguintes dicas podem contribuir para melhorar a sua vigilância em relação a este tipo de ataques.

Não abra e-mails e anexos de fontes suspeitas

Se não conhece o remetente em questão, não precisa de responder a um e-mail. Mesmo que os conheça e suspeite da sua mensagem, consulte e confirme as notícias de outras fontes, nomeadamente por telefone ou diretamente no site oficial de um prestador de serviços ou comerciante. Lembre-se que os endereços de e-mail podem ser falsificados; mesmo um e-mail supostamente vindo de uma fonte de confiança pode realmente ter sido iniciado por um intruso.

Utilize mecanismos de autenticação multifator

Uma das peças de informação mais valiosas que os atacantes procuram são as credenciais do utilizador. A utilização da autenticação multifator ajuda a garantir a proteção da sua conta em caso de compromisso do sistema, dado que, para além da habitual solicitação do nome de utilizador e da respetiva senha, recorre a um método complementar de verificação (por exemplo, através de um código de segurança enviado para o seu telemóvel). Fale com os responsáveis da sua entidade para disponibilizar esta funcionalidade, caso ainda não tenha acesso à mesma.

Desconfie de ofertas tentadoras

Se uma oferta soar muito sedutora, pense duas vezes antes de aceitá-la como facto. Ao procurar o tópico num motor de busca (p.e., o Google), pode rapidamente obter mais informação sobre se está efetivamente a lidar com uma oferta legítima ou uma armadilha.

Mantenha o software antivírus e *antimalware* atualizado

Certifique-se de que as atualizações automáticas estão ativadas e verifique periodicamente se as atualizações foram aplicadas e são efetuados diagnósticos (scans) regulares ao seu sistema para possíveis infeções. Caso tal não ocorra fale com o serviço que presta apoio informático à sua entidade.

V. Saiba lidar com esquemas de phishing através do e-mail

Se tem uma conta de e-mail, quase de certeza que já recebeu mensagens com tentativas de induzi-lo a fornecer informações pessoais, comprar produtos que não serão entregues ou clicar em links e ficheiros maliciosos. Estes e-mails podem assumir a forma de esquemas demasiado bons para serem verdadeiros (oportunidades de negócio/investimento, produtos de

cura ou perda de peso, ou lotarias/prémios), alertas de crise (ou alguém que procura ajuda ou indica que está em risco), ou "phishing" para obter informações pessoais, fazendo-se passar por uma instituição de confiança. Estas tentativas têm-se tornado cada vez mais sofisticadas. Os burlões podem criar e-mails convincentes, que parecem vir de fontes fidedignas, incluindo o seu banco, prestadores comerciais de serviços públicos e até mesmo entidades governamentais.
Seguindo as orientações abaixo reduzirá drasticamente o risco de ser vítima de fraudes por e-mail e phishing.

6.V.1 Como detetar uma mensagem de phishing?

Quando receber uma mensagem de e-mail, considere os pontos abaixo. Normalmente, uma mensagem de phishing apresenta algumas características que o devem colocar em alerta:

- A mensagem pede qualquer informação pessoal (senha, cartões de crédito, IBAN, números de identificação, etc.)?
- A mensagem pede informações sensíveis sobre outros indivíduos?
- A mensagem pede-lhe para abrir imediatamente um anexo?
- A mensagem contém links que aparentam apontar para sites credíveis?

Passe o rato sobre os links do e-mail sem carregar neles. O link de texto hover, que aparece na barra inferior do browser, corresponde ao que está visível no texto da mensagem? Os links reais são de um site com o qual normalmente teria de interagir? Veja com atenção!

Quando paira o cursor do rato sobre o link, sem carregar, parece que o link pertence à organização que envia a mensagem? Lembre-se que, em termos gerais, o site oficial da organização deve ser a última parte do nome de domínio, antes de qualquer subdiretório "/" (por exemplo, https://www.azores.gov.pt/email-phishing.html. Todavia, nalguns casos em que o software do agressor está envolvido, a última parte será o domínio dele (por exemplo, https://www.azores.gov.pt.**xyz**.me/email-phishing.html). Sob a pressão do dia-a-dia, em que é preciso fazer o trabalho depressa, é muito fácil cair neste tipo de

ataques se o olho do utilizador não estiver sensível e bem treinado. Veja se existem outros aspetos que evidenciem mensagens suspeitas:

- O endereço de e-mail "From (De)" parece-lhe pertencer a alguém que conhece, uma organização com quem interage ou uma conta de e-mail adequada?
- Clique em 'Responder' – O endereço no campo 'To (Para)' corresponde ao remetente da mensagem?
- Existem muitos destinatários a quem o e-mail é endereçado? Ou será que o campo dos destinatários está vazio, denotando possivelmente muitos destinatários em cópia cega (bcc/ blind cc)?
- A assinatura da mensagem está diferente - seja no conteúdo ou no formato gráfico - daquilo que estaria à espera?
- Não estava à espera de um e-mail desta natureza (por exemplo, redefinição de password, expiração da conta, transferência bancária, confirmação de viagem, valores por regularizar junto de prestadores de serviços públicos, etc.)?
- O e-mail é de uma entidade ou pessoa com quem nunca interagiu?
- É difícil chegar a uma conclusão sobre como o remetente obteve legitimamente o seu endereço de e-mail?
- A linguagem da mensagem está em português correto, compatível com os padrões de comunicação comercial ou institucional da suposta entidade remetente? Ou estará escrita num português que leve a suspeitar que possa ter sido escrito por um estrangeiro ou por um motor de tradução automática?

Se não tem a certeza da legitimidade de uma mensagem de correio eletrónico dirigida a um endereço do organismo, por favor, reporte a ocorrência ao serviço responsável pela prestação de apoio informático à sua entidade.

6.V.2 O que NÃO devo fazer

NÃO envie senhas ou informações confidenciais por e-mail

Nenhuma organização legítima lhe solicitará para enviar a sua senha, informação de conta, número de segurança social, dados bancários (incluindo IBAN ou dados de cartões com matrizes de códigos para validação de transações) ou outros dados confidenciais por e-mail.

NUNCA responda a um e-mail solicitando informações pessoais, financeiras ou outras informações protegidas, mesmo que pareça ser da organismo, do seu banco ou de outra instituição de confiança.

Em vez disso, reporte diretamente a ocorrência à instituição de onde o e-mail parece estar a vir, utilizando o número listado no seu cartão de crédito ou extrato bancário (ou documento equivalente, como a conta do seu telemóvel se o correio eletrónico alegar ser do seu operador de telecomunicações). Se o e-mail parecer ser do organismo, reencaminhe-o para o serviço de suporte interno competente, certificando-se de que inclui os cabeçalhos de e-mail completos.

NÃO clique em links para "verificar a sua conta" ou "login" em qualquer e-mail

Abra sempre uma nova janela e use a página oficial da instituição para iniciar sessão em qualquer conta.
Os links num e-mail podem parecer ir para o site fidedigno, mas na verdade podem estar a redirecioná-lo para uma página que rouba as suas informações de login.

NÃO responda, clique em links ou abra anexos em spam ou e-mail suspeito

Clicar ou responder a spam permite a verificação o seu endereço de e-mail, ficando os agressores a saber que aquela conta existe e está em uso ativo por uma pessoa (você). Isso incentiva mais tentativas deste tipo no futuro. Envie as mensagens de spam diretamente para o lixo ou reporte-o internamente. NUNCA abra anexos de remetentes que não conhece.

NÃO ligue para o número indicado num e-mail não solicitado nem dê dados confidenciais a um chamador

Os riscos associados ao phishing de e-mail aplicam-se igualmente às chamadas telefónicas e às mensagens por SMS, situações em que são conhecidas, respetivamente, por *vishing* (verbal+phishing) e *smishing* (sms+phishing). O phishing telefónico pode ser ainda mais difícil de detetar do que o phishing por e-mail. Os chamadores podem fazer-se passar por pessoal institucional, funcionários ou representantes de organismos que precisam da sua ajuda para completar cadastros e afins, ou mesmo agentes da polícia. Nunca dê informações sensíveis a uma pessoa que não conhece pessoalmente. Se a necessidade for legítima, poderá ligar de volta para a pessoa usando números fidedignos ou endereços de e-mail indicados no site institucional oficial.

6.V.3 O que devo fazer

Reportar o e-mail personificado ou suspeito

Se receber um e-mail a pedir informações pessoais, de login ou de contas financeiras e parecer ser do organismo, do seu banco ou de outra instituição de confiança, reencaminhe o e-mail para o serviço de suporte interno competente, tendo a certeza de incluir cabeçalhos de e-mail completos. Encaminhe também o e-mail para a organização que está a ser personificada. A maioria das organizações têm informações nos seus websites sobre onde relatar problemas. Pode começar por pesquisar no site por "proteção contra fraudes" ou "spam" para encontrar o endereço de e-mail correto.

Seja cauteloso sobre a abertura de anexos, mesmo de remetentes de confiança

As contas de e-mail podem ser pirateadas ou personificadas por burlões através de ficheiros anexos a mensagens de e-mail que tenham sido infetados com vírus e malware. Se abertos, estes podem aceder aos seus dados e/ou danificar o seu computador. Desconfie de abrir anexos não solicitados ou materiais para descarregar a partir de um e-mail, mesmo que pareçam vir de alguém que conhece. Em caso de dúvida sobre a legitimidade da mensagem, considere se a relevância do anexo vale potencialmente pôr em perigo os seus dados pessoais e os sistemas de informação do organismo.
Procure formas alternativas de obter a informação (cupão, documento, etc.) alegadamente anexadas. Tente obter a informação no site oficial do remetente. Se não conseguir encontrar a informação anexada em outro lugar, examine a extensão do ficheiro no anexo antes de abri-la. Se a extensão estiver entre as extensões listadas abaixo, é mais provável que seja maliciosa. (Atenção: Esta lista não é exaustiva.)

- ..exe
- .msi, .bat, .com, .cmd, .hta, .scr, .pif, .reg, .js, .vbs, .wsf, .cpl, .jar
- .docm, .xlsm, .pptm (pode conter macros).
- .rar, .zip, .7z

Note que nenhum tipo de ficheiro é 100% seguro, especialmente se o seu sistema operativo ou qualquer um dos seus programas e aplicações não tiverem sido devidamente atualizados. Considere verificar a legitimidade do e-mail e anexo com o remetente, antes de abri-lo.

Verifique a existência de programas antivírus e de firewall no seu computador

Os programas antivírus e de firewall podem protegê-lo de aceitar inadvertidamente ficheiros maliciosos, dado que detetam e bloqueiam, em tempo real, as tentativas de entrada de ficheiros infetados e ataques através da rede. Uma firewall ajuda a tornar o seu computador invisível na Internet e bloqueia todas as comunicações de fontes não autorizadas. É especial-

mente importante utilizar uma firewall se tiver uma ligação de banda larga. Se o seu dispositivo foi disponibilizado pelo organismo, é suposto já possuir estas componentes de segurança instaladas. Todavia, caso, por algum motivo, tal não tenha ocorrido, contate imediatamente o seu serviço e apoio informático do organismo.

Verifique regularmente os seus extratos bancários e de cartões de crédito

Analise periodicamente os movimentos das suas contas bancárias e dos cartões de crédito para ter a certeza de que todos as transações foram autorizadas por si. Solicite anualmente o seu mapa de responsabilidades de crédito junto do Banco de Portugal, para ter a certeza de que não há contas não autorizadas abertas em seu nome. Pode solicitar o seu mapa de responsabilidades de crédito, gratuitamente, no sítio web do Banco de Portugal, nesta localização: https://www.bportugal.pt/area-cidadao/formulario/227.

Proteja as suas informações pessoais

Quando estiver a fazer compras online, apenas partilhe dados do seu cartão de crédito ou outras informações pessoais quando estiver a lidar com uma empresa, e respetivo sítio web, que conhece e em quem confia. Todavia, mesmo as organizações mais credíveis, e por mais meios tecnológicos que possam ter ao seu dispor, estão sujeitas a riscos de cibersegurança, sendo que muitas delas têm sido atacadas com sérios impactos, inclusive algumas nacionais de renome. Em suma, ninguém está isento de poder vir a sofrer um ataque relevante. Neste sentido, evite, ao máximo, utilizar os dados dos seus cartões de crédito físicos. Porém, se o fizer, assegure-se, junto da respetiva entidade bancária emissora, de que qualquer transação está sujeita a uma operação de validação prévia através, por exemplo, do seu telemóvel. Alternativamente, como forma de simplificar a segurança das operações com cartões de crédito, procure utilizar cartões de crédito virtuais (serviço MBNET do seu banco), criados por si e associados a um valor de limite máximo. Poderá criar um cartão virtual MBNET para uma única compra, o que se afigura ser o mais seguro, dado que após essa transação

pontual, o cartão não poderá ser utilizado novamente. Por outro lado, se fizer uma subscrição anual de um serviço na Internet, com pagamentos recorrentes, por exemplo mensais, poderá subscrever um cartão virtual MB-NET que é válido para um único comerciante, mas que permite múltiplas transações durante um período máximo de 12 meses.

Saiba com quem está a lidar

Não faça negócios com nenhuma entidade que não forneça o seu nome, endereço de rua e número de telefone. Se for a primeira vez que recorre a essa empresa, obtenha informações sobre a mesma nos motores de busca, para perceber se existem indícios de que poderá estar perante uma potencial situação de fraude.

Não aja por impulso

Resista a qualquer desejo de "agir agora" apesar da oferta e dos termos. Cuidado com as janelas de pop-up que apresentam um tempo limite para poder "agarrar" um bom negócio ou que dizem que têm um telemóvel para si, porque é o 1.000.000º visitante. Assim que entregar o seu dinheiro, pode nunca mais recuperá-lo.

Leia as letras pequenas

Analise todas as condições da compra online, apresentadas por escrito, e reveja-as cuidadosamente antes de fazer um pagamento ou assinar um contrato.

VI. Utilize frases-passe para proteger a sua conta

Uma frase-passe é uma sequência de palavras, números ou símbolos usados para iniciar a sessão na sua conta do organismo. As frases-passe são

mais seguras do que as palavras-passe porque contêm mais caracteres e também podem ser mais fáceis de lembrar do que as palavras-passe, se estiverem associadas a um tema ou ideia secretos.

6.VI.1 Quais são os requisitos de uma frase-passe?

Recomendamos a utilização de uma frase curta como palavra-passe. A sua frase deve conter pelo menos 12 caracteres (no máximo 127 caracteres), devendo conter uma combinação de caracteres maiúsculos, minúsculos, números e outros especiais.

6.VI.2 Como posso manter a minha senha segura?

O que é secreto, deve manter-se secreto

Ninguém no organismo, ou em qualquer outro lugar, deve pedir a sua senha por qualquer motivo, seja pessoalmente ou via telefone, chat, e-mail, correio postal ou online de qualquer forma. Se duvidar da autenticidade de qualquer mensagem de correio eletrónico ou website, ou estiver preocupado com a segurança da sua conta, contacte o serviço de suporte interno competente, logo que seja possível.

6.VI.3 Dicas para reforçar a segurança da palavra-passe

Para conseguir reforçar a segurança das suas senhas, siga as seguintes orientações:

1. Altere as palavras-passe, pelo menos, de três em três meses para utilizadores sem privilégios de administração e 45-60 dias para contas de administrador;
2. Utilize senhas diferentes para contas diferentes;
3. Evite contas genéricas usadas por várias pessoas e senhas partilhadas;

4. Escolha frases-passe desafiantes que incluam uma combinação de letras (maiúsculas e minúsculas), números e caracteres especiais (por exemplo, <$>, <%> e <&>).
5. Reveja a qualidade das suas senhas, à luz das boas práticas descritas neste manual e atue em conformidade. Peça ajuda internamente, se necessitar;
6. Evite informações pessoais, tais como datas de nascimento, nomes de animais de estimação e de figuras públicas;
7. Utilize palavras-passe ou frases-passe de mais de 12 caracteres;
8. Utilize um cofre de senhas onde precisará de memorizar apenas a senha principal;
9. Não utilize a função de preenchimento automático de palavras-passe de um navegador.

Como já referido anteriormente, uma dica de segurança de senha avançada consiste no uso da autenticação de dois fatores, que é uma forma de os websites confirmarem a identidade de um utilizador. Após iniciar sessão com sucesso, recebe uma mensagem de texto com um código para, em seguida, introduzi-lo para autenticar o seu ID. Esta abordagem requer que os utilizadores não só conheçam as suas palavras-passe como também tenham acesso ao seu próprio telemóvel. A autenticação de dois fatores funciona bem porque os cibercriminosos raramente roubam a senha e o telefone de um utilizador final ao mesmo tempo. Os principais bancos e instituições financeiras permitem a autenticação de dois fatores por defeito mas se, no seu caso, não o estiverem a fazer, deve solicitá-lo.

VII. Utilização das redes sociais

6.VII.1 Problemas de privacidade e segurança

Muito do que a Internet sabe sobre si, sabe-o através das redes sociais. Sabe o quanto partilhou? Certifique-se de que as configurações das suas contas e a sua forma de comunicar protegem a sua privacidade e segurança e refletem a imagem pública e profissional que pretende projetar.

6.VII.2 Ajuste os seus perfis e configurações nas redes sociais

Navegue pelos perfis das suas contas nas redes sociais e elimine quaisquer conteúdos publicados, relativamente aos quais agora perceba que poderá ter ido longe demais. Remova o seu endereço de casa (liste apenas a sua cidade, se alguma coisa) e a sua data de nascimento (pelo menos tire o ano de nascimento). Tenha em mente que as suas publicações e fotos mais antigas, que outrora lhe pareciam bem, poderão não se adequar atualmente às suas identidades pessoal e profissional. Por outro lado, as publicações mais antigas dos seus "amigos" ainda poderão estar visíveis e continuar a identificar ou mencionar o seu perfil, quando aparece nas fotos deles, se não tiver ajustado as suas definições de privacidade para as ocultar.

6.VII.3 Dicas de Segurança para Redes Sociais

Os sites das redes sociais, tais como o Facebook e o Twitter, podem ser uma ótima maneira de se conectar com amigos ou conhecidos. Mas há algumas dicas de segurança que deve ter sempre em mente.

Adeque as suas definições de privacidade

Aprenda a usar e otimizar as definições de privacidade e segurança nas suas redes sociais. Isto ajuda-o a controlar quem vê o que publica e a gerir a sua experiência online de forma positiva. Tenha em atenção que as definições de privacidade desses sites podem mudar sem que se aperceba disso, pelo que convém efetuar uma validação regular das mesmas.

Proteja a sua reputação nas redes sociais

Recorde: uma vez publicado, sempre publicado. O que publica online fica online. Pense duas vezes antes de publicar conteúdos que não gostaria que os seus familiares, colegas ou futuros empregadores vissem. Pesqui-

sas recentes descobriram que 70% dos recrutadores rejeitaram candidatos com base em informações que encontraram online.

Construa uma reputação online positiva

Tenha em atenção que os recrutadores respondem a uma marca pessoal forte e positiva online. Então demonstre o seu domínio e profissionalismo na sua área de competência.

Mantenha as informações pessoais confidenciais

Tenha cuidado com a quantidade de informações pessoais que divulga nas redes sociais. Quanto mais informação publicar, mais fácil será alguém usar essa informação para roubar a sua identidade, aceder aos seus dados ou cometer outros crimes, tais como engenharia social ou perseguição.

Utilize senhas fortes

Certifique-se de que a sua palavra-passe ou frase-passe tem pelo menos doze caracteres de comprimento e consiste nalguma combinação de letras, números e caracteres especiais (por exemplo, +, @, # ou $). Relembre o que falámos na secção Utilize frases-passe para proteger a sua conta.

Utilize a autenticação de dois fatores (Two-factor authentication – 2FA)

A autenticação de dois fatores (2FA) é um método de segurança de gestão de identidade e acesso que requer duas formas de identificação para aceder a recursos e dados. Para além da autenticação convencional por palavra-passe ou frase-passe, recorra a um método complementar para completar o processo de autenticação, de preferência, com recurso a um segundo dispositivo físico.

Seja cauteloso nas redes sociais

Mesmo os links que parecem que vêm de amigos podem, por vezes, conter software prejudicial ou fazer parte de um ataque de phishing. Se suspeitar, não clique. Contacte primeiro o seu amigo para verificar a validade do link. Suspeite igualmente dos pedidos de dinheiro de amigos, através das redes sociais ou de serviços de chat, tais como o WhatsApp e Telegram, pois geralmente são originados por hackers que usurparam a conta de um conhecido. Esteja atento a certas nuances, como alterações na forma habitual de escrita de conhecidos, pois muitos hackers estrangeiros usam motores de tradução online para gerarem frases em português que não "soam" bem.

VIII. Navegação segura na Internet

6.VIII.1 Os principais perigos na utilização de um navegador

Quando alguém se aventura na Internet, é fácil envolver-se na vasta teia de ameaças que espreitam em muitas páginas web. Algumas são facilmente detetadas, mas outras estão bem dissimuladas.

É particularmente importante ter em atenção o *malvertising* – uma forma de código malicioso que distribui *malware* através de publicidade online – que pode estar escondido dentro de um anúncio, incorporado numa página do site ou agregado com downloads de software. Este tipo de ameaça pode ser exibido em qualquer site, mesmo aqueles que aparentam ser mais confiáveis.
Também precisa de ter cuidado com os esquemas das redes sociais. Os hackers criaram um parque infantil de obstáculos virtuais em todos os principais sites de redes sociais. Alguns dos ataques mais comuns no Facebook incluem técnicas de *click-jacking*, esquemas de *phishing*, páginas falsas, aplicações fraudulentas e o infame e persistente *worm Koobface*, que dá aos atacantes o controlo do computador da vítima enquanto replicam o ataque a todos na sua lista de contatos no Facebook.

O Twitter também não é imune a questões de segurança. Uma vez que o site de microblogging é simultaneamente uma rede social e um motor de busca, coloca problemas extra. De acordo com o CNET News, apenas 43% dos utilizadores do Twitter poderiam ser classificados como utilizadores "verdadeiros" em comparação com os outros 57%, reputados como utilizadores "questionáveis". Entre as coisas a ter em conta no Twitter estão mensagens diretas que levam a esquemas de phishing e URLs encurtados que escondem intenções maliciosas.

6.VIII.2 Boas práticas na utilização de um navegador web

Como forma de reforçar as suas condições de segurança quando navega na Internet, siga as seguintes práticas:

- Seja conservador com as descargas (downloads) online. Tenha cuidado por onde clica;
- Tenha cuidado com as fraudes antivírus, designadamente com os sites que oferecem scans de vírus online e de forma gratuita;
- Aceda apenas a sites bem conhecidos e respeitáveis;
- Confirme que cada site é genuíno e não um site fraudulento;
- NUNCA se registe num site qualquer com o mesmo login/e-mail e senha da sua conta de e-mail do organismo nem de outras contas de e-mail que possua;
- Determine se o site utiliza o protocolo de segurança SSL, uma tecnologia de segurança para estabelecer ligações encriptadas entre servidores Web e navegadores. Para confirmar isso, veja se na barra de endereços do seu navegador, o URL começa com "https://". Se sim, estará a usar SSL;
- Não entre em sites que, no primeiro acesso, o navegador indica que o certificado de segurança não é válido ou está expirado;
- Não clique em links em e-mails — de preferência, vá diretamente a sites.

IX. As redes *peer-to-peer* (P2P) e os seus riscos

As redes *peer-to-peer* (P2P) permitem que os utilizadores partilhem ficheiros online através da comunicação informal entre computadores que executam o mesmo software.
Todos os dias, milhões de pessoas partilham ficheiros online. Seja música, jogos ou software, a partilha de ficheiros pode dar às pessoas acesso a uma grande quantidade de informação. Para partilhar ficheiros através de uma rede P2P, descarrega-se software especial que liga o seu computador a outros computadores que executam o mesmo software. Milhões de utilizadores podem estar ligados uns aos outros através deste software de cada vez. O software é geralmente gratuito.
É promissor, mas certifique-se de que avalia bem os prós e os contras. A partilha de ficheiros pode ter vários riscos. Por exemplo, quando estiver ligado a programas de partilha de ficheiros, pode, sem saber, permitir que outros copiem ficheiros privados, até mesmo dar acesso as estruturas inteiras de pastas que nunca pretendeu partilhar. Por outro lado, ao partilhar material protegido por legislação de direitos autorais, corre o risco de incorrer em problemas legais. Poderá ainda descarregar inadvertidamente ficheiros infetados com vírus, facilitar a exploração de falhas de segurança no seu computador ou descarregar involuntariamente pornografia rotulada como outra coisa.
Tenha em atenção que a distribuição não autorizada de material protegido por direitos de autor, incluindo a partilha de música, filmes e software com direitos de autor, através de aplicações *peer-to-peer* como sejam o BitTorrent, Emule, PopcornTime, entre outros, é considerada uma atividade ilícita e pode sujeitar o prevaricador a sanções legais, nomeadamente:

- Ter de indemnizar o titular dos direitos de autor como resultado de um processo judicial;
- Ter de pagar as despesas do titular dos direitos de autor e os honorários do advogado que conduziu o processo em tribunal;
- Todas as penalidades previstas na lei, mesmo que da partilha de ficheiros não tenha decorrido vantagem económica ;
- Apreensão de material informático.

Tenha igualmente em conta que, na eventualidade de terem sido usados recursos informáticos e/ou de comunicações da organismo, poderão ser aplicadas sanções e instaurados processos disciplinares, nos termos da legislação aplicável.

X. Segurança de laptops e dispositivos móveis

Talvez o seu computador já possua todo o software de segurança necessário e já utilize mecanismos de autenticação robustos, como senhas muito difíceis de adivinhar e mecanismos de dupla autenticação. Talvez até já encripte os seus dados e seja atento para não se deixar enganar por e-mails que tentam obter os seus dados pessoais. Mas e o portátil em si? Uma pequena distração é tudo o que é preciso para o seu equipamento desaparecer. Se isso acontecer, pode perder mais do que uma peça de hardware cara.
O facto é que a informação potencialmente sensível e valiosa que reside no seu portátil pode ser um íman para um ladrão de identidades.
É provável que tenha ouvido histórias sobre portáteis roubados nas notícias ou de amigos e colegas. Ninguém pensa que o portátil deles será roubado — pelo menos até encontrarem a bagageira do carro arrombada ou repararem que o seu portátil desapareceu enquanto foi deixado a carregar numa mesa do café do aeroporto e virou as costas para pedir mais um café.
Os smartphones e tablets tornaram-se tão populares para comunicar com colegas e contactos pessoais (já para não falar de tirar fotografias, jogar, ouvir música, ver vídeos e navegar com GPS). Infelizmente, a portabilidade e a função destes dispositivos móveis para todos estes fins podem torná-los alvos privilegiados para ladrões e hackers .
Com vista a proteger os seus dispositivos e a informação neles contida, siga os conselhos indicados abaixo. A sua forma de estar deve basear-se sempre numa atitude de prevenção.

Bloqueie o seu dispositivo com uma senha

Configure o telefone ou o tablet para bloquear o ecrã automaticamente após um breve período de inatividade. Esta é a primeira linha de defesa – se alguém quer aceder ao dispositivo, primeiro precisa de decifrar o código. Esta não é uma tarefa fácil e pode funcionar como um fator dissuasor contra o roubo.

Configure a opção de limpeza automática do dispositivo

Configure o seu dispositivo para apagar automaticamente o seu conteúdo, após a ocorrência de um número repetido de tentativas falhadas na inserção do código de desbloqueio. A maioria dos dispositivos pode ser configurada para apagar os seus dados após um número predefinido de tentativas falhadas de código de acesso (por exemplo, 10). Uma vez que os seus dados são apagados é quase impossível para um ladrão ou hacker recuperá-lo. O backup frequente dos seus dados irá protegê-lo se o dispositivo for roubado, ou se o perder ou danificar.
Todavia, se optar por ativar esta opção, não deixe depois o seu telefone nas mãos de uma criança pequena que, sem se aperceber, ao tatear no ecrã bloqueado, poderá desencadear uma limpeza completa e inconveniente ao conteúdo do dispositivo.
Se o seu computador portátil pertencer ao organismo, confirme com o seu serviço interno de suporte se o conteúdo do mesmo poderá ser remotamente apagado, em caso de furto ou roubo, dado que o Windows suporta esta funcionalidade através do MDM (*Mobile Device Management*). Através do MDM é possível impor o uso de determinados códigos de acesso e aplicar funcionalidades de *geofencing* que permitem que um dispositivo perdido seja mais facilmente localizado.

Evite ao máximo as estações de carregamento públicas com tomadas USB

Utilize sempre os seus próprios cabos e transformador para carregar o dispositivo. Alguns hackers roubam informações ou carregam código

malicioso nos equipamentos das vítimas, criando quiosques com cabos de carga que estão ligados a computadores invisíveis.

Mantenha sempre os seus dispositivos debaixo de olho

NUNCA deixe os seus dispositivos sem supervisão e cuidado com os telemóveis em cima da mesa, nos restaurantes ou qualquer outro lugar público, enquanto come ou conversa. Uma breve distração e lá vai o telemóvel... Mantenha-o fora de vista dos olhos dos amigos do alheio. Uma técnica frequentemente usada por redes de criminosos é enviar adolescentes às mesas e mostrar um cartão em formato A5 com um pedido de ajuda escrito. Ao apresentar o cartão à frente da pessoa, o telefone fica encoberto por breves instantes e discretamente retirado, enquanto a vítima fica distraída a tentar perceber o que está escrito no papel.

Utilize ferramentas de localização remota

Várias soluções de software ajudam a localizar dispositivos perdidos ou roubados através de GPS e capacidades de *geofencing*. A Apple oferece um serviço como este para dispositivos móveis chamados *Find my iPhone*. Para os utilizadores Android, o *Android Device Manager* também oferece estes serviços. Da mesma forma, muitas aplicações de terceiros estão disponíveis em cada uma das lojas de aplicações.

Mantenha os seus dispositivos limpos

Os telefones são minicomputadores, e tal como os computadores "grandes", precisam de ser limpos de vez em quando. Usar um scanner antivírus e *malware* é sempre uma boa ideia. O *malware* pode comprometer a informação armazenada em dispositivos móveis e tem um efeito bola de neve que se acumula continuamente até que este abrande ou pare o dispositivo.

7. Recursos recomendados

I. Cursos de cibersegurança online gratuitos

O Centro Nacional de Cibersegurança (CNCS) oferece um conjunto de cursos online gratuitos, para que qualquer cidadão possa adquirir competências básicas em cibersegurança. Estes cursos abordam vários temas, como as principais ameaças no ciberespaço, os cuidados a ter na utilização das tecnologias, o problema da desinformação ou o que fazer para consumir online de forma segura, entre outros.

Cidadão Ciberseguro

O Cidadão Ciberseguro é um curso de e-learning curto, simples e acessível ao cidadão/colaborador em geral, com o intuito de o dotar de conhecimentos que permitam proteger-se e adotar boas práticas de ciber-higiene em diferentes contextos diários, incluindo no local de trabalho.

Cidadão Ciberinformado

O curso de e-learning Cidadão Ciberinformado destina-se a qualquer cidadão que procure aprender a identificar notícias falsas e a verificar a veracidade da informação consultada online, evitando a partilha de desinformação e contribuindo para um ciberespaço verdadeiramente democrático.

Consumidor Ciberseguro

Através do curso de e-learning Consumidor Ciberseguro os formandos poderão obter conhecimentos que lhes permitam proteger-se e adotar boas práticas quando realizam compras online, evitando de modo mais eficaz a burla e o roubo de credenciais de cartões de crédito, por exemplo. Com este curso cada um poderá fazer compras online com mais segurança.

Cidadão Cibersocial

O curso de e-learning Cidadão Cibersocial é uma iniciativa do Centro Internet Segura, coordenado pelo Centro Nacional de Cibersegurança. Trata-se de um curso interativo, que procura ser apelativo para todas as pessoas que queiram saber como utilizar as redes sociais de um modo mais seguro e protegendo a sua privacidade.

II. Boas práticas de cibersegurança

O CNCS oferece também um conjunto vasto de informações, recomendações e boas práticas para que o cidadão saiba como proceder perante as ameaças da cibersegurança.

Glossário

Antimalware – Programa de computador utilizado para prevenir, detetar e remover software malicioso.

Ataques de Negação de Serviço – Também conhecidos pela sigla em inglês DOS (Denial-Of-Service), constituem tentativas de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Os servidores web são os alvos típicos. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga.

Banner – Faixas promocionais de uso comum em presenças web. Constituem uma forma de pubicidade na Internet com o intuito de levar o utilizador a realizar uma ação, usualmente envolvendo clicar no banner para seguir para uma página web específica previamente definida pelo anunciante.

Click-jacking – Técnica maliciosa de induzir o utilizador a clicar em algo diferente do que o utilizadorusuário percebe, potencialmente revelando informações confidenciais ou permitindo que outras pessoas assumam o controle doe seu computador enquanto clicam em objetos aparentemente inócuos, incluindo páginas da web.

Geofencing - Serviço baseado em GPS que define limites geográficos virtuais, enviando uma notificação ou alerta quando o dispositivo entra ou sai da área definida.

Link de texto *hover* – Refere-se à hiperligação que surge na parte inferior do ecrã do navegador quando passa o rato sobre texto hiperligado.

Malware - Software malicioso. É qualquer software intencionalmente feito para causar danos a um computador, servidor, cliente, ou a uma rede de computadores.

Patches - P rograma de computador criado para atualizar ou corrigir um software de forma a melhorar sua usabilidade ou performance.

Peer-to-peer - em português, ponto a ponto ou P2P é uma arquitetura de redes de computadores onde cada um dos pontos, ou nós, da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central ou hierarquia.

Pop-up – Elemento que emerge automaticamente durante a navegação num sítio web, sem que o utilizador tenha realizado ação nesse sentido. Pode ser, por exemplo, um banner pop-up, ou seja, uma faixa com uma mensagem publicitária que surge a dado momento durante a navegação do utilizador.

Ransomware - Ransomware é um tipo de malware de sequestro de dados, feito por meio de criptografia, que torna reféns os arquivos pessoais da própria vítima e cobra resgate (ransom) para restabelecer o acesso a estes arquivos. O resgate é cobrado em criptomoedas, o que, na prática, torna quase impossível rastrear o criminoso.

SMS – Short-Message-System. Em português, serviço de mensagens curtas. É um serviço disponível em telemóveis digitais que permite o envio de mensagens curtas, popularmente conhecidas como mensagens de texto.

Spam – Spam de email refere-se a mensagens de correio eletrónico não solicitadas e enviadas massivamente por email.

Texto claro (Cleartext) – Refere-se a informação armazenada ou enviada de forma não encriptada. A informação encontra-se no estado legível e consumível.

Worm – Refere-se a software malicioso que se replica com o objetivo de se espalhar para outros computadores. Geralmente, o Worm usa uma rede de computadores para se espalhar, ou mesmo unidades USB, contando com falhas de segurança no computador de destino. Alguns worms também se alastram por mensagens de e-mail, criando anexos maliciosos que depois enviam para as listas de contato da conta invadida.

GOVERNO
DOS **AÇORES**

https://portal.azores.gov.pt

PRR
Plano de Recuperação e Resiliência

GOVERNO
DOS **AÇORES**

REPÚBLICA
PORTUGUESA

Financiado pela
União Europeia
NextGenerationEU