

---

# POLÍTICA DE SEGURANÇA

---

Política que os colaboradores devem respeitar para o tratamento de dados pessoais. Recomendações que os colaboradores devem adotar em conjunto com a empresa.

Se precisar de mais informações, entre em contacto com o Responsável de Segurança.



---

O responsável pelo tratamento **Santa Casa da Misericórdia de Ferreira do Alentejo** com o **NIPC 500851719**, sede em **Rua da Eira, N.º 13, Apartado 83, 7900-195 Ferreira do Alentejo**.

COLOCA À DISPOSIÇÃO DO UTILIZADOR EM BAIXO INDICADO

AS SEGUINTEs POLÍTICAS DE TRATAMENTO DE DADOS

- A. Política de proteção no posto de trabalho
- B. Política de utilização do correio eletrónico
- C. Política de palavras-passe
- D. Política de Wi-Fi e redes externas
- E. Política de utilização de dispositivos móveis não corporativos
- F. Política de utilização de dispositivos móveis corporativos
- G. Política de aplicações permitidas
- H. Política de armazenamento na cloud
- I. Política de armazenamento nos equipamentos de trabalho
- J. Política de armazenamento em dispositivos amovíveis
- K. Política de eliminação segura e gestão de suportes
- L. Política de controlo de acessos
- M. Política de resposta a incidentes
- N. Política de cópias de segurança

ACEITAÇÃO E COMPROMISSO DE CUMPRIMENTO

Mediante a assinatura deste documento, o utilizador reconhece que leu e compreendeu todas as políticas de tratamento e está consciente da sua responsabilidade e obrigatoriedade de cumprimento.

Ferreira do Alentejo, \_\_\_\_\_ de \_\_\_\_\_

NOME		ASSINATURA
APELIDOS		
NIF		

## A. Proteção no Posto de Trabalho

A gestão da informação empresarial é efetuada, fundamentalmente, a partir do posto de trabalho, tanto a partir de dispositivos tecnológicos como de forma mais tradicional (papel, telefone, etc.). Daí a importância de o funcionário ter consciência e responsabilizar-se pelo cumprimento de determinadas normas para a segurança do seu posto.

Por um lado, o funcionário deve conhecer os riscos não tecnológicos, por exemplo:

- ✓ a informação em papel ao alcance de pessoas não autorizadas;
- ✓ a falta de confidencialidade dos meios de comunicação tradicionais;
- ✓ o perigo de roubo ou extravio dos dispositivos amovíveis (pen drives, discos rígidos externos, etc.);
- ✓ o acesso físico de terceiros às zonas de trabalho (distribuidores, pessoal da limpeza, etc.).

Por outro lado, em muitos postos de trabalho tem-se acesso a computadores, dispositivos móveis e portáteis com ligação à rede da empresa e ao exterior (Internet). Assim, constituem uma "porta de entrada" para a empresa e para os seus recursos de informação. É fundamental que o funcionário tenha consciência do que isto implica para evitar acidentes que possam ter origem no seu posto de trabalho, acentuados por desconhecimento ou por falta de preparação:

- ✓ acessos não autorizados aos computadores e a partir destes, a aplicações da empresa; ataques por malware;
- ✓ roubo e fuga de dados em formato digital;
- ✓ ataques de engenharia social, isto é, enganos para manipular a vítima para obter informação (credenciais, informação confidencial, etc.) ou para conseguir que executem alguma ação em sua representação (instalar um programa, enviar e-mails, efetuar algum acesso, etc.).

Para garantir uma utilização adequada dos dispositivos e meios do local de trabalho e para minimizar o impacto que todos estes riscos podem ter para a empresa, deve-se implementar uma política de proteção do posto de trabalho. A seguir, apresenta-se uma série de obrigações e boas práticas em matéria de segurança que se aplicam ao posto de trabalho.

O objetivo é garantir a segurança de toda a informação e dos recursos geridos no posto de trabalho.

Num	MEDIDA	ENTENDO
A1	Destruidora avançada de documentação: a informação confidencial obsoleta que já não seja útil deve ser destruída de forma segura, tendo em conta o método apropriado para cada suporte de armazenamento.	
A2	Bloqueio programado da sessão: deve programar-se o bloqueio automático da sessão nos equipamentos para quando não é detetada atividade do utilizador durante um curto período de tempo (máximo 15 minutos)	

A3	Sistema operativo atualizado: os sistemas operativos dos equipamentos informáticos devem ser mantidos atualizados. Caso seja necessário, solicite apoio do pessoal técnico.	
A4	Antivírus atualizado e ativo: o antivírus deve ser mantido atualizado e ativo em todos os equipamentos informáticos	
A5	Utilização de meios de armazenamento: a informação deve ser armazenada em dispositivos autorizados e de forma segura.	
A6	Proibição de alteração: não é permitido alterar a configuração do equipamento ou instalar aplicações não autorizadas. A instalação de software específico ou a alteração da configuração de equipamentos, caso seja necessário para o desempenho do trabalho, deve ser sempre solicitado ao pessoal da informática.	
A7	Política de mesas limpas: a mesa de trabalho deve estar sempre desobstruída e sem documentação confidencial, nem dispositivos amovíveis, ao alcance de outras pessoas.	
A8	Destruição básica de documentação: devem utilizar-se destruidoras de papel para eliminar a informação confidencial.	
A9	Detenção de documentação sensível: os documentos enviados para impressão devem ser imediatamente recolhidos e depois de digitalizada a informação deve ser guardada, principalmente se se tratar de informação sensível.	
A10	Não revelar informação a utilizadores não devidamente identificados: deve verificar-se, prévia e corretamente, o destinatário dos dados, tendo em conta os perigos da engenharia social e a informação que não deve ser revelada.	
A11	Obrigações de confidencialidade: o utilizador de dados deve aceitar e cumprir a política de confidencialidade que assinou ao integrar um posto de trabalho.	
A12	Detenção de palavras-passe: as palavras-passe não devem ser publicadas, nem partilhadas. Também não devem ser anotadas em documentos, agendas, nem em qualquer outro tipo de suporte.	
A13	Utilização de palavras-passe fortes: devem ser utilizadas palavras-passe difíceis de decifrar, que incluam, pelo menos, 8 caracteres, incluindo maiúsculas, minúsculas, números e caracteres especiais (1, @, +, ], ?, etc.).	
A14	Alteração periódica das palavras-passe: as palavras-passe devem ser alteradas, pelo menos, de 6 em 6 meses.	

A15	Obrigatoriedade de bloquear a sessão e desligar o equipamento: é obrigatório bloquear a sessão ao ausentar-se do posto de trabalho e desligar o equipamento no final do dia de trabalho.	
A16	Notificação de incidentes: é obrigatório notificar qualquer incidente de segurança (vírus, perda de informação ou de dispositivos, etc.)	

## **PONTOS-CHAVE DA POLÍTICA DE SEGURANÇA NO POSTO DE TRABALHO**

Os funcionários também serão informados sobre outras políticas relacionadas com equipamentos ou serviços que utilizem no seu trabalho: correio eletrônico, armazenamento, etc.

**Destruição avançada de documentação através de mecanismos seguros** - A informação obsoleta será destruída de forma segura, de acordo com a Política de eliminação segura e gestão de suportes. Em concreto:

- ✓ mediante destruidoras de papel disponíveis para os funcionários;
- ✓ contratando um serviço externo de destruição segura, notificando os funcionários sobre a sua existência e obrigatoriedade de utilização, (Caso seja Pertinente);
- ✓ dando a conhecer os riscos associados à utilização de caixotes de lixo para documentos sensíveis (dados pessoais, informação financeira, etc.).

**Bloqueio programado da sessão** - O pessoal da informática programará o bloqueio automático da sessão nos equipamentos para quando não é detetada atividade do utilizador num curto período de tempo. Adicionalmente, pode ponderar-se a programação do desligamento geral dos equipamentos após o término da atividade empresarial.

**Sistema operativo atualizado** - O pessoal responsável pelos sistemas aplicará a Política de atualizações de software, revendo periodicamente os equipamentos para garantir a sua atualização, ou ativando as atualizações automáticas.

**Antivírus atualizado e ativo** - O pessoal responsável pelos sistemas aplicará a Política antimalware que incluirá a instalação e a atualização de ferramentas antimalware em todos os equipamentos e sistemas, bem como a sua revisão periódica de forma a garantir a proteção antimalware.

**Segurança de impressoras e equipamentos auxiliares do escritório** - O pessoal responsável verificará que as impressoras e outros equipamentos ligados à rede, ou que possam conter informação da empresa, estão incluídos nas Políticas de segurança:

- ✓ estarão dentro do perímetro da firewall, caso exista;
- ✓ o acesso ao seu painel de configuração será efetuado por palavra-passe e por canais codificados;
- ✓ se tiverem Wi-Fi a sua segurança será configurada;
- ✓ se tiverem discos rígidos, as Políticas de armazenamento serão revistas.

**Utilização de meios de armazenamento** - Para que o funcionário faça uma utilização correta dos dispositivos de armazenamento disponíveis, deve conhecer e aplicar a legislação corporativa relativa ao armazenamento local no equipamento de trabalho, armazenamento na rede corporativa, na cloud e nos dispositivos amovíveis.

**Proibição de alteração da configuração do equipamento e de instalação de aplicações não autorizadas** - Constitui um risco permitir que o funcionário altere a configuração do equipamento ou instale as aplicações que considerar necessárias. Esta alteração poderá ter consequências de infeção de equipamentos e, portanto, de perda de informação. Se o funcionário precisar de uma configuração ou de um software específico para o desempenho do seu trabalho deverá solicitá-lo formalmente à equipa do departamento informático, ou empresa autorizada.

**Política de mesas limpas** - Compreendemos como política de mesas limpas a obrigação de guardar a documentação de trabalho ao ausentar-se do posto de trabalho e ao terminar a jornada laboral. Não deve deixar-se informação sensível à vista de pessoas que possam fazer uma utilização indevida da mesma. O cumprimento desta política implica:

- ✓ manter o posto de trabalho limpo e organizado;
- ✓ guardar a documentação e os dispositivos amovíveis que não estejam a ser utilizados nesse momento e, principalmente, ao ausentar-se do posto de trabalho no final da jornada laboral;
- ✓ não registar nomes de utilizador, nem palavras-passe em blocos de notas ou similares.

**Não abandonar documentação sensível em impressoras ou scanners** - Para evitar que a informação acabe em mãos indesejadas, o utilizador deve:

- ✓ recolher, imediatamente, os documentos enviados para impressão; guardar a documentação depois de digitalizada;
- ✓ utilizar os mecanismos de impressão segura caso estejam disponíveis.

**Não revelar informação a utilizadores não devidamente identificados** - A informação é um dos ativos empresariais com valor mais elevado. Por este motivo, é possível que alguém tente obter parte desta informação (palavras-passe de utilizadores, informação de contas bancárias, etc.) enganando um funcionário. Esta prática é conhecida como engenharia social.

Os infratores fazem-se passar por um responsável, pessoa ou empresa conhecida para que o funcionário confie e disponibilize a informação que é solicitada utilizando para tal uma chamada telefónica, um e-mail, as redes sociais ou mensagens tipo SMS ou WhatsApp.

**Obrigação de confidencialidade** - O funcionário deve aceitar um acordo de confidencialidade relativo a qualquer informação à qual tenha acesso no decorrer da sua participação laboral na empresa. A obrigação de confidencialidade terá validade durante todo o tempo que seja exigido pelo contrato laboral. A informação deve ser protegida mesmo quando o funcionário já não fizer parte da empresa.

**Utilização de palavras-passe** - O utilizador deve respeitar a Política de palavras-passe:

- ✓ as credenciais (nome de utilizador e palavra-passe) são confidenciais e não podem ser publicadas, nem partilhadas;
- ✓ as credenciais não devem ser anotadas em documentos, nem em qualquer outro tipo de suporte;
- ✓ as palavras-passe devem ser fortes: pelo menos 8 caracteres incluindo maiúsculas, minúsculas, números e caracteres especiais (!, @, +, ], ?, etc.);
- ✓ devem ser alteradas periodicamente.

**Obrigatoriedade de bloquear a sessão e desligar o equipamento** - Para evitar o acesso indevido ou por pessoal não autorizado ao equipamento do posto de trabalho:

- ✓ o funcionário deverá bloqueá-lo sempre que se ausentar do seu posto de trabalho;
- ✓ o funcionário desligará o equipamento ao terminar a jornada laboral.

**Obrigatoriedade de notificar incidentes de segurança** - O funcionário deve comunicar qualquer incidente relacionado com o seu posto de trabalho:

- ✓ alertas de vírus/malware gerados pelo antivírus;
- ✓ chamadas suspeitas recebidas a solicitar informação sensível; mensagens de correio eletrónico que contenham vírus;
- ✓ perda de dispositivos móveis (portáteis, smartphones ou tablets) e dispositivos de armazenamento externos (USB, CD/DVD, etc.);
- ✓ eliminação accidental de informação;
- ✓ alteração accidental de dados ou registos nas aplicações com informação crítica; comportamentos anómalos dos sistemas de informação;
- ✓ descoberta de informação em localizações não designadas para tal;
- ✓ evidência ou suspeita de acesso físico de pessoal não autorizado a áreas de acesso restrito ( gabinetes, armazéns, etc.);
- ✓ evidência ou suspeita de acessos não autorizados a sistemas informáticos ou a informação confidencial por parte de terceiros;
- ✓ qualquer atividade suspeita que possa ser detetada no seu posto de trabalho.



## **B. POLÍTICA DE UTILIZAÇÃO DO CORREIO ELETRÓNICO**

O correio eletrónico é uma ferramenta de comunicação imprescindível para o funcionamento de uma empresa. Os seus benefícios são evidentes: acessibilidade, rapidez, possibilidade de enviar documentos anexos, etc., embora quando foi criado não foi feito a pensar nas suas aplicações atuais, nem na segurança.

Como qualquer ferramenta de comunicação corporativa, é necessário definir a sua utilização correta e segura visto que, para além de abusos e de erros não intencionais na sua utilização que possam provocar um prejuízo à empresa, o correio eletrónico converteu-se num dos meios utilizados pelos cibercriminosos para efetuar os seus ataques.

Os funcionários podem enviar, por erro, documentos confidenciais a quem não deveriam, podem revelar, sem querer, o endereço de correio eletrónico (que é um dado pessoal) de clientes ou utilizadores, ou utilizar o seu endereço corporativo para usos não permitidos.

Também é habitual que nas caixas de entradas de endereços profissionais chegue spam, e-mails de phishing que tentam roubar credenciais ou e-mails que substituem entidades ou pessoas. Nestes casos, utilizam-se técnicas de engenharia social para conseguir os objetivos maliciosos, por exemplo: infetar, roubar credenciais ou obtenção de dados confidenciais. Num e-mail malicioso, tanto o remetente como o assunto, o corpo, os anexos ou as ligações incluídas podem ser elaborados de forma a enganar o destinatário da mensagem. Para evitar cair na armadilha dos cibercriminosos devemos, além de utilizar meios tecnológicos (antivírus, antimalware, antispam, etc.), consciencializar os nossos funcionários para que saibam distinguir estas mensagens.

Para evitar os riscos associados à utilização do e-mail empresarial devemos consciencializar os funcionários para que façam uma utilização segura do mesmo e informá-los sobre as normas que regulam as condições e as circunstâncias em que podem ser utilizados, bem como as possíveis sanções e ações a implementar no caso de se detetar uma utilização indevida.

O objetivo é estabelecer normas de utilização permitida e segura do correio eletrónico empresarial que sirvam para impedir erros, incidentes e utilizações ilícitas e para evitar ataques por esta via.

Num	MEDIDA	ENTENDO
B1	Antimalware e antispam: tanto o servidor como o servidor de correio eletrónico devem dispor de aplicações antimalware e antispam instaladas e ativadas	
B2	Codificação e assinatura digital: deve utilizar-se tecnologia de codificação e assinatura digital que possa ser utilizada com o correio eletrónico para proteger a informação confidencial e garantir a autenticidade da empresa enquanto remetente, (Certificados SSL).	

B3	Desativar elementos não seguros: deve desativar-se o formato HTML, a execução de macros e a transferência de imagens para uma proteção adicional das contas de correio eletrónico.	
B4	Ocultar os endereços de correio eletrónico: os endereços de correio eletrónico corporativos não devem ser publicados em páginas Web, nem em redes sociais sem utilizar técnicas de ofuscação.	
B5	Utilização adequada do e-mail corporativo: nunca se deve utilizar o e-mail corporativo para fins pessoais e o conteúdo deve cumprir as regras definidas pela empresa, isto é, assuntos estritamente profissionais.	
B6	E-mails suspeitos: deve suspeitar-se da autenticidade do e-mail quando a mensagem: apresenta alterações de aspeto, contém um "apelo à ação" urgente, convida ou solicita a realização de algo que não é habitual ou solicita credenciais de acesso a uma página Web ou aplicação (conta bancária, ERP, etc.)	
B7	Identificação do remetente: os remetentes devem ser identificados antes de abrir um e-mail. Se se suspeitar de substituição do remetente, este deve ser contactado por outro meio para o confirmar.	
B8	Análise de anexos: os anexos dos e-mails de remetentes desconhecidos devem ser cuidadosamente analisados antes de serem abertos. Se se suspeitar da sua autenticidade, não devem ser descarregados, nem abertos.	
B9	Verificação de ligações: as ligações incluídas nos e-mails devem ser cuidadosamente verificadas antes de aceder às mesmas.	
B10	Não responder ao spam (correio lixo): nunca se deve corresponder a e-mails de spam. Devem ser incluídos na lista de spam e eliminados.	
B11	Utilizar a cópia oculta (BCC): quando se envia e-mails para diversos endereços deve utilizar-se a cópia oculta.	
B12	Reenvio de e-mails: no caso de necessitar de reenviar um e-mail corporativo para uma conta pessoal deve solicitar-se previamente autorização à direção da empresa.	
B13	Evitar redes públicas: não se deve consultar e-mails corporativos quando se está ligado a redes públicas como Wi-Fi de hotéis, restaurantes ou aeroportos.	

## *PONTOS-CHAVE DA POLÍTICA DE UTILIZAÇÃO DE E-MAIL CORPORATIVO*

**Normativa de utilização do correio eletrónico** - A empresa terá uma normativa relativa ao uso do correio eletrónico que o funcionário aceitará ao ingressar no seu posto de trabalho. Este será informado sobre a proibição de utilização do e-mail corporativo com fins pessoais que não estejam relacionados com a empresa. O conteúdo do e-mail deverá cumprir com a normativa e a sua utilização inadequada poderá acarretar sanções. O e-mail corporativo pode ser supervisionado pela direção da empresa, incluindo uma cláusula na normativa assinada pelo funcionário.

**Antimalware e antisspam** - De acordo com a Política antimalware, deve instalar aplicações antimalware e ativar os filtros antispam tanto no servidor, como no cliente de e-mail. Estes filtros permitirão que os e-mails maliciosos sejam identificados e não cheguem à caixa de entrada evitando assim a sua possível abertura.

**Utilização adequada do e-mail corporativo** - O funcionário conhece e aceita a normativa relativa à utilização do e-mail corporativo.

**Palavra-passe segura** - Todas as contas devem utilizar palavras-passe de acordo com a Política de palavras-passe, recomenda-se:

- ✓ utilizar uma palavra-passe segura para evitar acessos não autorizados; utilizar um fator de autenticação duplo para as contas críticas;
- ✓ se se aceder ao e-mail através de uma interface Web nunca se assinalará a opção de memorização da palavra-passe.

**E-mails suspeitos** - Os funcionários devem aprender a identificar correios fraudulentos e suspeitar quando:

- ✓ o corpo da mensagem apresentar alterações de aspeto (logótipos, rodapé, etc.) relativamente às mensagens recebidas anteriormente desse mesmo remetente;
- ✓ a mensagem contém um "apelo à ação" urgente que incentiva ou convida a fazer algo que não é habitual;
- ✓ forem solicitadas credenciais de acesso a uma página Web ou aplicação (conta bancária, ERP, etc.).

**Identificação do remetente** - O funcionário não abrirá qualquer e-mail sem identificar o remetente. Se o remetente não for um contacto conhecido será necessário prestar especial atenção visto que se pode tratar de um novo cliente ou de um e-mail malicioso.

Se o remetente for um contacto conhecido, mas por outros motivos (corpo da mensagem, ficheiros anexos, ligações, etc.) suspeitar que a identidade do remetente possa ter sido substituída, deve contactar o mesmo por outro meio para confirmar a sua identidade.

**Análise de anexos** - Ao receber uma mensagem com um anexo, este deve ser cuidadosamente analisado antes de abrir. Embora o remetente seja conhecido pode ter sido substituído sem que nos apercebamos.

**Verificação de ligações** - Ao receber uma mensagem com uma ligação, antes de clicar o destinatário deve:

- ✓ rever o URL, posicione-se sobre o texto da ligação para visualizar o endereço antes de

- clicar no mesmo;
- ✓ identificar ligações suspeitas que pareçam ligações legítimas observando que podem ter: letras ou caracteres a mais ou a menos e passar despercebidos;
- ✓ podem estar a utilizar homógrafos, isto é, caracteres que são parecidos em determinadas fontes (1 e l, O e 0).

**Utilizar a cópia oculta (BCC)** - Ao enviar mensagens a diversos destinatários, envie-as para si próprio e utilize a opção de cópia oculta (BCC na maioria dos clientes de e-mail), em vez da cópia normal, CC. A cópia oculta impede que os destinatários vejam a quem mais o mesmo e-mail foi enviado. Desta forma evitaremos que qualquer pessoa possa ter acesso a uma série de endereços de e-mail válidos para os quais possam enviar spam ou mensagem fraudulentas. Lembre-se de que o endereço de correio eletrónico é um dado pessoal dos nossos clientes e utilizadores, que não devemos utilizar para outros fins que não aqueles para os quais foi solicitado. Não devemos divulgá-lo ou comunicá-lo a terceiros sem o seu consentimento.

**Reenvio de e-mails** - Informar-se-á sobre a proibição de reenvio de e-mails corporativos para contas pessoais, salvo casos excecionais que devem ser autorizados pela direção.

**Evitar as redes públicas** - Evitar utilizar o correio eletrónico a partir de ligações públicas (o Wi-Fi de um café, o computador de um hotel, etc.) de acordo com a Política de utilização de Wi-Fi e de ligações externas visto que o nosso tráfego de dados pode ser interceptado por qualquer utilizador desta rede. Como alternativa, é preferível utilizar redes de telemóvel como 3G ou 4G.

### C. POLÍTICA DE PALAVRA-PASSE

O tratamento diário da informação da empresa requer o acesso a diferentes serviços, dispositivos e aplicações para os quais utilizamos o par de credenciais: nome de utilizador e palavra-passe. Para segurança dos serviços e sistemas nos quais existem contas de utilizadores, temos de garantir que as credenciais de autenticação são geradas, atualizadas e revogadas de forma ideal e segura.

Dentro da gestão de palavras-passe inclui-se o dever de difundir e garantir o cumprimento de boas práticas: atualizá-las regularmente, garantir a sua força (dificuldade para as adivinhar ou corromper), não utilizar palavras-passe predefinidas ou como fazer a sua custódia.

O objetivo é estabelecer, difundir e verificar o cumprimento de boas práticas na utilização de palavras-passe.

NUM	MEDIDA	ENTENDO
C1	Gestão de palavras-passe: deve definir-se um sistema avançado de gestão de palavras-passe que contemple todos os aspetos relativos ao seu ciclo de vida.	
C2	Ferramentas para garantir a segurança das palavras-passe: deve recorrer a técnicas e a ferramentas informáticas para garantir a segurança das palavras-passe, (caso se aplique).	
C3	Não utilizar palavras-passe por defeito: as palavras-passe predefinidas que estão incluídas para acesso a aplicações, equipamentos e sistemas devem ser alteradas.	
C4	Fator duplo para serviços críticos: devem incluir-se sistemas de autenticação multifator nos acessos a serviços com informação muito sensível, (caso se aplique).	
C5	Não partilhar as palavras-passe com ninguém: As palavras-passe são individuais, pelo que devem ser mantidas em segredo e deve evitar-se partilhá-las. Se se suspeitar de que houve uma violação da integridade de uma palavra-passe, a situação deve ser imediatamente reportada.	
C6	As palavras-passe devem ser fortes: as palavras-passe devem ser geradas tendo em conta a sua força.	
C7	Não utilizar a mesma palavra-passe para serviços diferentes: deve certificar-se de que seleciona palavras-passe diferentes para cada um dos serviços que utiliza.	
C8	Alteração periódica das palavras-passe: as palavras-passe devem ser alteradas periodicamente, pelo menos, de 6 em 6 meses.	
C9	Não utilizar a opção de lembrar palavras-passe: não deve utilizar nunca as opções de memorização de palavras-passe dos navegadores e aplicações.	

## **D. POLÍTICA DE WI-FI E REDES EXTERNAS**

É habitual ter de aceder aos dados da empresa quando estamos fora do local de trabalho (viagens, reuniões, teletrabalho, etc.). Em determinadas ocasiões, não podemos utilizar as redes ou as ligações 4G/5G, o que nos obriga a estabelecer ligação a redes domésticas ou a redes públicas (hotéis, cafés, aeroportos, etc.) que na maioria dos casos pode não ser segura.

É prudente assumir que, por defeito, as redes sem fios utilizadas pelos trabalhadores fora do local de trabalho não dispõem das medidas de segurança necessárias para a proteção dos dados e das comunicações corporativas. Frequentemente, a informação confidencial da nossa empresa é transmitida através de redes sem fios cuja segurança não está sob o nosso controlo pelo que, antes de utilizar estas redes, nos devemos certificar de que os dados viajam convenientemente protegidos.

A empresa deve estabelecer as condições e as circunstâncias nas quais se permite o acesso remoto aos serviços corporativos. Isto é, determinar quem pode aceder a quê, como e quando. Esta tarefa implica dispor dos meios necessários para desenvolver e disponibilizar a formação correspondente aos trabalhadores para que saibam como fazer a ligação de forma segura e como manter os seus equipamentos seguros quando viajam ou estabelecem ligação a partir do exterior.

Uma das ferramentas de segurança que podemos implementar para efetuar acessos remotos corporativos a partir do exterior da empresa é a utilização de uma Rede Privada Virtual ou VPN. Utilizamos uma VPN quando precisarmos de aceder a informação confidencial de forma remota e a rede que estivermos a utilizar não oferecer garantias suficientes de segurança.

Apenas deve utilizar redes Wi-Fi públicas seguras se não tiver outra forma mais segura (redes móveis 4G/5G ou uma VPN) disponível para executar atividades de alto risco (utilização de e-mail, trabalhar com documentos online, redes sociais, banca online ou compras online) certificando-se, todavia, que acede a páginas Web legítimas, codificadas (<https://>) e com certificado.

**Redes sem fios dos dispositivos móveis** - Ativar a ligação Wi-Fi, Bluetooth ou antena GPS apenas na altura em que as for utilizar e com as adequadas medidas de segurança.

**Utilização de dispositivos móveis** - Se utilizar dispositivos móveis para trabalhar fora da empresa, é necessário tomar as medidas de segurança indicadas nas Políticas de utilização de dispositivos móveis corporativos e na política de utilização de dispositivos móveis não corporativos.

**Utilização de computadores não corporativos** - Se utilizar computadores de uso público, evite executar atividades de alto risco (utilização de e-mail corporativo, trabalhar com documentos online, redes sociais, banca online ou compras online). Desconfie da segurança do equipamento e das suas ligações. De qualquer forma, se tiver necessidade de os utilizar para efetuar login em algum serviço corporativo sempre que este for permitido e não puder utilizar uma VPN:

- ✓ reveja o espaço envolvente para evitar olhares de observadores ou de câmaras;
- ✓ utilize o modo de navegação privada do navegador;
- ✓ digite o URL ou o endereço Web, em vez de utilizar o motor de busca;
- ✓ verifique se a página à qual acede é autêntica, se utiliza o protocolo <https://> e se tem certificado e este se encontra em vigor;
- ✓ evite que o navegador guarde as palavras-passe;
- ✓ ao terminar a sessão limpe o histórico de navegação e os cookies no navegador;
- ✓ não ligue pen drives, nem outros dispositivos externos;
- ✓ certifique-se de que não deixa qualquer ficheiro pessoal no equipamento.

Se utilizar computadores domésticos:

- ✓ atualize o software de sistemas operativos e aplicações; utilize um utilizador não partilhado;
- ✓ instale e ative um antivírus e a firewall do sistema operativo;
- ✓ não instale aplicações sem licença ou cuja origem desconheça.

## **E. POLÍTICA DE UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS NÃO CORPORATIVOS**

A utilização de dispositivos pessoais (portáteis, smartphones, tablets), propriedade do funcionário, no âmbito corporativo é denominada de BYOD (Bring Your Own Device). Trata-se de uma prática muito frequente, portanto deve prestar-se especial atenção para que a sua utilização não comprometa a segurança da informação da empresa.

Uma vez estabelecida a política de segurança relativa à utilização segura dos dispositivos pessoais para o trabalho, os funcionários devem ser informados sobre a mesma e devem aceitá-la antes de utilizarem os seus dispositivos para aceder a aplicações ou tratar informação da empresa.

O objetivo é estabelecer as normas que garantam a segurança da informação se se permitir a utilização dos dispositivos pessoais no âmbito corporativo.

NUM	MEDIDA (CASO SE APLIQUE)	ENTENDO
E1	Normas e procedimentos BYOD: Apenas se permite a utilização de dispositivos não corporativos se tiverem antivírus e sistema operativos atualizados, se tiverem configurações de segurança, se não tiverem software instalado sem licença e se estiverem devidamente encriptados. Não obstante, deve dispor-se de autorização específica por parte do pessoal responsável.	
E2	Limitação do acesso a redes externas: proíbe-se a utilização de redes sem fios externas não corporativas para o acesso aos sistemas da entidade através de equipamentos não corporativos. Apenas são permitidos acessos de redes 3G/4G.	
E3	Lista de aplicações não permitidas: antes de instalar uma aplicação num dispositivo não corporativo para utilização de dados da entidade, deve solicitar-se autorização ao pessoal responsável.	
E4	Processo de eliminação da informação: quando se deixar de utilizar para usos corporativos um dispositivo pessoal, ou quando o funcionário que o utilizava sair da empresa, devem ser previamente formatados para evitar a recuperação de dados.	
E5	Controlo de acesso à rede: é boa prática o acesso à rede corporativa com equipamentos não corporativos através da utilização de ligações VPN.	
E6	Controlo de utilizadores e dispositivos: deve certificar-se de que você e o seu dispositivo estão registados na listagem de utilizadores e dispositivos autorizados.	
E7	Encriptação dos dispositivos: a utilização de dispositivos não corporativos deve ser codificada e as pastas com dados corporativos devem ser protegidas com palavras-passe.	
E8	Extravio de dispositivos: os dispositivos não corporativos devem ser configurados com medidas de segurança para proteger a informação corporativa (localização, bloqueio do ecrã, eliminação remota de dados e acompanhamento das aplicações executadas) em caso de extravio.	
E9	Desconexão do Wi-Fi e Bluetooth: deve desativar-se a procura de redes Wi-Fi e de dispositivos através de Bluetooth quando não forem necessários.	



## **PONTOS-CHAVE DA POLÍTICA DE UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS NÃO CORPORATIVOS**

**Conscientização dos funcionários** - Os dispositivos como o telemóvel ou o portátil são suscetíveis de roubo. Assim, é importante envolver os utilizadores na proteção dos seus próprios dispositivos, conscientizando-os da importância da proteção do mesmo e dos dados que contém.

**Sensibilização dos funcionários** - Proporcionaremos aos funcionários informação suficiente para uma utilização segura dos dispositivos. Por exemplo:

- ✓ configurar os parâmetros de segurança dos dispositivos;
- ✓ atualizar, periodicamente, tanto o sistema operativo como as aplicações (em especial, o antivírus);

A ligação de dados do seu telemóvel deverá ser apenas 3G/4G e quando as redes sem fios disponíveis forem desconhecidas, essas redes Wi-Fi devem ser consideradas inseguras.

**Lista de aplicações não recomendadas** - Estabeleceremos uma lista de tipos de aplicações que não poderão ser instaladas nestes dispositivos devido ao perigo que implicam para a informação corporativa. Estas aplicações podem requerer, para a sua instalação, acesso a dados confidenciais da organização (dados da agenda, geolocalização do terminal, etc.).

**Controlar o armazenamento de dados corporativos** - As aplicações pessoais nos dispositivos móveis para o tratamento de dados na cloud não são tão seguras como as empresariais pelo que é necessário prestar especial atenção a este intercâmbio de ficheiros. Pode permitir-se a consulta de informação na cloud, mas não se recomenda a atualização da mesma a partir destes dispositivos pessoais.

**Processo de eliminação da informação** - Recomendações para entregar/eliminar a informação nestes dispositivos quando o funcionário sair da empresa.

**Controlo de acesso à rede** - O acesso à rede corporativa através de dispositivos pessoais deve estar integrado no sistema de controlo de acessos (autenticação,...). Desta forma, o funcionário deve acreditar a sua identidade antes de aceder aos serviços da rede corporativa. Para maior segurança da empresa pode proporcionar aos seus funcionários acesso através da rede privada virtual (VPN) que codifica as comunicações.

**Controlo de utilizadores e dispositivos** - Deve existir um registo de utilizadores e dispositivos que têm acesso aos dados e aplicações da empresa, incluindo informação detalhada dos privilégios de segurança atribuídos para autorizar o acesso tanto a esses utilizadores como aos dispositivos.

Aplicar medidas técnicas para garantir um armazenamento seguro da informação nos dispositivos. Por exemplo:

- ✓ Implementar nos dispositivos mecanismos de codificação da documentação, para além dos de autenticação de utilizadores.
- ✓ Impedir a gravação automática das credenciais de utilizadores associadas às ferramentas corporativas.

**Bloqueio programado** - Configura o dispositivo para que bloqueie automaticamente após um período de inatividade.

**Extravio de dispositivos** - Perante a possibilidade de perda ou extravio deste tipo de dispositivos, estabelecer as seguintes medidas:

- ✓ Localização através de GPS, Wi-Fi ou informação da antena de telefone com a qual o dispositivo estiver ligado. Depois de assinalado como "perdido", o Smartphone começa a enviar os dados da sua localização de forma permanente para uma conta previamente

configurada (e-mail, SMS, central de controlo,...).

- ✓ Ter o bloqueio de ecrã do terminal sempre ativado. Caso contrário, será bloqueado de forma remota.
- ✓ Eliminação remota de dados: esta opção permite que os dados incluídos no dispositivo sejam eliminados de forma remota, impedindo a sua utilização por um utilizador não legítimo.
- ✓ Vigiar as aplicações que são executadas. O seguimento das chamadas efetuadas e as redes sociais acedidas, entre outros, costumam ser dados suficientes para obter nomes, apelidos e até mesmo o endereço de um possível infrator.
- ✓ Desconexão do Wi-Fi e Bluetooth. Deve desativar-se no telefone a procura de redes Wi-Fi e de dispositivos através de Bluetooth quando não forem necessários.

## **F. POLÍTICA DE UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS CORPORATIVOS**

Hoje em dia, é possível trabalhar fora das instalações corporativas com a utilização de dispositivos móveis (portáteis, tablets e telemóveis) propriedade da empresa ou do funcionário.

As tecnologias de mobilidade, como os computadores portáteis, permitem ao funcionário desempenhar o seu trabalho como se estivesse nas instalações da empresa: acesso ao e-mail, às aplicações corporativas, a informação confidencial, etc.

Estes dispositivos são mais suscetíveis a perda ou roubo pelo que existe um risco acrescido no acesso à informação corporativa. Assim, é imprescindível implementar algumas medidas de segurança como estabelecer palavras-passe de acesso fortes, codificar a informação armazenada, manter o equipamento sempre atualizado e com o antivírus ativo, etc.

Se a empresa permitir ao funcionário utilizar os seus próprios dispositivos (BYOD o Bring Your Own Device) deve consultar a Política de utilização de dispositivos móveis não corporativos para que a utilização seja efetuada com garantias de segurança.

O objetivo é estabelecer uma normativa de segurança aplicável nos níveis de gestão, técnico e de utilizador, para uma correta utilização dos dispositivos móveis corporativos.

NUM	MEDIDA	ENTENDO
F1	Atribuição de dispositivos: existe um pedido e atribuição de dispositivos móveis corporativos.	
F2	Registo de equipamentos: todos os equipamentos portáteis atribuídos devem ser registados (qual o portátil e a quem é atribuído), bem como o software e o hardware de que o funcionário precisa.	
F3	Manutenção de dispositivos: para efetuar alterações no dispositivo (modificação de hardware, instalação de software, alterações na configuração), estas devem ser solicitadas ao pessoal responsável.	
F4	Proteção da Bios: a BIOS dos equipamentos portáteis deve ser configurada através de palavras-passe	
F5	Software de localização: alguns equipamentos precisam de software de localização.	
F6	Armazenamento da informação: não se deve armazenar informação corporativa que não seja estritamente necessária para o desenvolvimento do trabalho.	
F7	Tratamento de informação confidencial: a informação confidencial deve ser codificada e eliminada de forma segura.	
F8	Conexão a redes: apenas se deve ligar o portátil a redes conhecidas e privadas e optar por uma ligação 3G/4G quando as restantes redes disponíveis não forem fiáveis.	
F9	Notificação em caso de infeção: deve notificar-se o pessoal técnico responsável sobre a suspeita de infeção por vírus ou outro software malicioso do equipamento.	

F10	Transporte e custódia: não deve expor o equipamento a altas temperaturas. Não se deve negligenciar o portátil se se viajar em transportes públicos, não se deve guardar no carro, nem deixá-lo visível ou facilmente acessível. Se se trabalhar em locais onde não se garanta a sua custódia, deve ser bloqueado com um cadeado de segurança ou guardado num armário de segurança. Em caso de roubo ou perda do equipamento, deve notificar-se imediatamente o responsável.	
F11	Utilização do posto de trabalho. Devem ser aplicadas as normas reunidas na Política de utilização do posto de trabalho relativas à utilização de um equipamento informático (obrigação de notificar incidentes de segurança, utilização correta de palavras-passe, bloqueio do equipamento, etc.)	
F12	Responsabilidades. O funcionário conhece as responsabilidades associadas à utilização de dispositivos corporativos móveis e aplica as normas de segurança correspondentes.	

*PONTOS-CHAVE DA POLÍTICA DE UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS NÃO CORPORATIVOS*

**Atribuição de dispositivos** - Deve existir um procedimento de solicitação e atribuição dos dispositivos móveis corporativos para manter um inventário ativo e registar as necessidades dos trabalhadores.

**Registo de equipamentos** - É aconselhável manter um registo dos dispositivos móveis atribuídos (que dispositivo e a quem é atribuído). Também registar a utilização dada ao dispositivo, bem como o software e o hardware de que o funcionário precisa.

**Manutenção de dispositivos** - A manutenção de dispositivos fica restrita ao departamento responsável pela sua manutenção. Portanto, deve proibir-se que o utilizador faça alterações no hardware, instale software ou modifique a configuração do equipamento sem autorização do departamento competente.

**Software de localização** - No caso de se considerar necessário instalar ou ativar algum software de localização, tal será comunicado ao utilizador do dispositivo antes de efetuar a entrega do mesmo. O utilizador que vai estar sob geolocalização deve assinar um documento a aceitar esta condição.

**Armazenamento da informação** - A informação corporativa que não seja estritamente necessária para o desenvolvimento das tarefas do utilizador não deve ser armazenada no dispositivo. Se se aceder a informação a partir de vários dispositivos, esta tem de estar sincronizada para evitar duplicações e erros nas versões.

**Tratamento da informação confidencial** - Toda a informação confidencial deve ser armazenada codificada. Antes da devolução do dispositivo, a informação deve ser eliminada de forma segura ou deve solicitar-se a sua eliminação ao técnico responsável.

**Conexão a redes** - As conexões a redes alheias à organização seguirão as normas estabelecidas na política de utilização corporativa de redes externas.

O utilizador deve impedir que se possa aceder à informação armazenada no mesmo. Em caso algum se deve negligenciar o portátil quando se viaja em transportes públicos. Também não deve ser guardado no carro, nem deixado num local visível ou de fácil acesso. Se se trabalhar em locais onde não se garanta a custódia do equipamento, este deve ficar bloqueado com um cadeado de segurança ou guardado num armário de segurança. Em caso de roubo ou perda do equipamento, deve notificar-se imediatamente o pessoal técnico responsável.

**Utilização do posto de trabalho** - O utilizador aplicará as normas reunidas na Política de utilização do posto de trabalho que sejam relativas à utilização de um equipamento informático (obrigação de notificar incidentes de segurança, utilização correta das palavras-passe, bloqueio do equipamento, etc.).

**Responsabilidades** - O utilizador é responsável pelo equipamento portátil ou telemóvel que lhe é disponibilizado para desempenho das suas tarefas fora das instalações corporativas. Portanto, é o trabalhador que deve garantir a segurança tanto do equipamento, como da informação que contém. Esta normativa será de cumprimento obrigatório e poderá ser objeto de acordos assinados ao aceitar a utilização destes dispositivos.

## **G. POLÍTICA DE APLICAÇÕES PERMITIDAS**

As normas de proteção da propriedade intelectual obrigam as empresas a utilizar sempre software legal. A utilização de software pirata ou adquirido de forma fraudulenta poderia implicar sanções económicas e penais. Além disso, a instalação e a utilização de software ilegal em qualquer dispositivo aumentam os riscos de infeção por malware.

O objetivo é controlar que se utiliza sempre software autorizado na empresa e que este foi adquirido de forma legal.

NUM	MEDIDA	ENTENDO
G1	Registo de licenças: deve existir um registo atualizado das licenças disponíveis do software autorizado.	
G2	Competência de instalação, atualização e eliminação: apenas o pessoal técnico tem autorização para se encarregar da instalação, atualização e eliminação do software nos equipamentos corporativos.	
G3	Sanções por usos não autorizados: a empresa pode estabelecer uma política de sanções pelo uso não autorizado de software.	

## H. POLÍTICA DE ARMAZENAMENTO NA CLOUD

São muitos os motivos para armazenar informação corporativa na cloud:

- Aceder a informação a partir de qualquer dispositivo e lugar;
- Redução de custos e poupanças;
- Disponibilizar diretórios partilhados com diferentes permissões de acesso;
- permitir o trabalho corporativo sobre um documento.

Mas, antes da sua implementação na empresa, devem também ser avaliados os seus aspetos negativos como a dependência de terceiros ou a necessidade de ligação à Internet para ter acesso à informação.

Para que os funcionários façam um bom uso dos recursos de armazenamento, a empresa terá uma política de classificação da informação na qual se deve indicar que tipo de informação pode ser carregado para a cloud. Para além disso, informar-se-á o pessoal sobre o conteúdo da mesma.

Juntamente com esta classificação, deve existir uma normativa interna para o tratamento da informação crítica e sensível, que indicará quando deve ser codificada e outras medidas de segurança que serão aplicadas como backups ou eliminação segura da informação.

O objetivo é estabelecer em que casos se permite a utilização do armazenamento na cloud e manter de forma segura a informação armazenada na cloud, especificando regras, critérios e procedimentos que devem ser cumpridos por todos os funcionários que utilizem estes serviços.

NUM	MEDIDA	ENTENDO
H1	Utilização de serviços de armazenamento em clouds públicas: apenas se permite a utilização de serviços de armazenamento em clouds públicas autorizadas pela entidade.	
H2	Lista de serviços cloud permitidos: solicite ao responsável a lista de serviços de armazenamento na cloud que são ou não permitidos.	
H3	Processo de eliminação da informação na cloud: para a eliminação de dados armazenados na cloud deve ter-se em conta que também é necessário esvaziar o caixote de lixo do serviço de armazenamento, bem como todas as cópias localizadas nos equipamentos sincronizados, incluindo os caixotes de reciclagem dos referidos equipamentos.	
H4	Tipo de informação armazenada e tratamento: toda a informação crítica, confidencial ou sensível deve ser codificada antes de ser armazenada na cloud, ou se não for possível deve-se verificar a pertinência de colocar a informação na cloud.	
H5	Contratação de serviços de armazenamento na cloud: os serviços de armazenamento na cloud contratados pela entidade devem cumprir com os critérios organizativos e de segurança estabelecidos na normativa de proteção de dados em vigor. A decisão não compete ao utilizador.	

## **I. POLÍTICA DE ARMAZENAMENTO NOS EQUIPAMENTOS DE TRABALHO**

No posto de trabalho, os funcionários utilizam como ferramenta equipamentos informáticos: computadores, tablets, telemóveis, etc. Também geram e transmitem informação necessária para o desempenho das suas funções. Por vezes, esta informação é armazenada de forma local nos discos rígidos destes equipamentos, pelo que surge a necessidade de dispor de uma política que regule o procedimento para o fazer de forma segura. De igual modo, devem ser reguladas as políticas de armazenamento em dispositivos amovíveis, na cloud e na rede corporativa.

A empresa deverá uma política de classificação da informação. Juntamente com esta classificação elaborar-se-á um processo para o tratamento da informação crítica e sensível (de acordo com o RGPD), que indicará quando deve ser codificada, quando se tem de controlar o acesso à mesma e outras medidas de segurança a implementar como as cópias de segurança ou a destruição da informação.

O objetivo é manter de forma segura a informação armazenada de forma local, especificando regras, critérios e procedimentos que devem ser respeitados por todos os funcionários.

NUM	MEDIDA	ENTENDO
I1	O que pode ser armazenado nos equipamentos de trabalho: unicamente informação estritamente necessária para o trabalho que está a ser realizado no momento.	
I2	Onde guardar a informação: deve respeitar-se a árvore de diretórios de trabalho no servidor ou no computador, principalmente dados confidenciais e sensíveis.	
I3	Codificação da informação: a informação crítica e sensível deve ser codificada antes de ser guardada localmente, caso se aplique.	
I4	Conhecimento e aplicação da normativa. O pessoal deve conhecer e aplicar o processo estabelecido para o armazenamento no equipamento de trabalho.	



**PONTOS-CHAVE DA POLÍTICA DE ARMAZENAMENTO EM EQUIPAMENTOS DE TRABALHO**

**O que pode ser armazenado nos equipamentos corporativos** - Os funcionários devem saber qual o tipo de informação que pode ser armazenado nos equipamentos locais.

Pode-se elaborar um procedimento, que deve indicar, detalhadamente, onde guardar a informação relacionada com o trabalho dentro da árvore de diretórios do equipamento. Esta medida facilita a migração desta informação para os servidores.

**Conservação da informação em discos locais** - Para evitar problemas de espaço nos discos rígidos, estabelecer um período de tempo de conservação da informação. Decorrido este tempo, de acordo com a informação em questão, teremos de decidir se esta será transferida para os servidores empresariais ou se será definitivamente eliminada, caso se aplique.

**Codificação da informação** - O funcionário deve saber quando e como utilizar a codificação da documentação, de acordo com a política de utilização de técnicas criptográficas. Esta medida é útil em caso de fuga de informação ou acesso não autorizado, caso se aplique.

**Conhecimento e aplicação do procedimento** - Os funcionários devem conhecer e aplicar o procedimento relativo ao armazenamento no local nos seus equipamentos de trabalho e outras políticas relacionadas.

## J. POLÍTICA DE ARMAZENAMENTO EM DISPOSITIVOS AMOVÍVEIS

Os dispositivos de armazenamento amovíveis (unidades de memória USB, discos rígidos portáteis, cartões de memória, CD, etc.) permitem uma transferência rápida e direta de informação. Atualmente, são imprescindíveis e muito utilizados. Devemos aplicar as medidas de segurança que este tipo de dispositivos requer pela sua suscetibilidade ao roubo, manipulação, extravio e infeção por vírus.

A empresa deve decidir se permite o uso de dispositivos de armazenamento externos e, se assim for, deve dispor de uma normativa que contemple em que situações podem ser utilizados e que tipo de informação pode ser guardada nos mesmos.

Se for necessário armazenar informação sensível ou confidencial, serão utilizados dispositivos externos corporativos devidamente protegidos, serão armazenados em locais seguros e, caso ocorram incidentes (roubo, perda, infeção do dispositivo, etc.), o responsável será informado.

No caso de ser permitido o uso de dispositivos pessoais (dispositivos amovíveis da propriedade do funcionário) serão aplicadas as normas de segurança reunidas na política correspondente.

Para garantir a informação incluída nos dispositivos amovíveis, teremos de aplicar medidas de segurança como: codificar os dados armazenados, estabelecer permissões de acesso, alterar periodicamente a palavra-passe, etc.

Outro dos aspetos importantes a ter em conta é a eliminação da informação armazenada. Para garantir que os dados não voltarão a estar acessíveis, devemos utilizar os métodos de eliminação segura: destruição física do dispositivo, desmagnetização ou *overwrite* (substituição), conforme aplicável em cada um dos casos.

Em suma, devemos aplicar as medidas de segurança que este tipo de dispositivos requeira, bem como consciencializar os funcionários para a sua boa utilização. Desta forma protegeremos tanto a informação incluída nos mesmos como a dos dispositivos aos quais são ligados.

O objetivo é estabelecer normas de utilização dos dispositivos amovíveis que garantam a segurança da informação corporativa que armazenam e a dos equipamentos aos quais são ligados.

NUM	MEDIDA	ENTENDO
J1	Alternativas aos meios de armazenamento amovíveis. Sempre que possível, deve evitar-se o uso de dispositivos de armazenamento amovíveis e optar por meios alternativos (repositórios comuns ou pastas partilhadas, serviços cloud autorizados, etc.).	
J2	Registo de utilizadores e dispositivos: deve existir uma lista atualizada dos dispositivos amovíveis autorizados, utilizadores atribuídos e informação que armazenam, pelo que não devem ser utilizados dispositivos amovíveis não inventariados.	
J3	Medidas técnicas para garantir o armazenamento seguro: devem ser aplicadas medidas para o armazenamento seguro da informação no dispositivo amovível (codificação de dados, autenticação, alteração periódica de palavras-passe, etc.).	
J4	Medidas técnicas para garantir um armazenamento seguro da informação nos documentos: devem ser aplicadas medidas para o armazenamento seguro da informação nos documentos que são transferidos (controlo de acessos, decodificação, etc.).	

## ***K. POLÍTICA DE ELIMINAÇÃO SEGURA E GESTÃO DE SUPORTES***

Quando a informação deixa de ser necessária para a organização, chega à última fase do seu ciclo de vida e é necessário destruí-la de forma segura. Esta opção é indispensável se queremos que a informação não volte a estar acessível e que cumpra com a Lei de Proteção de Dados, quando incluir dados de caráter pessoal.

Também devemos utilizar a eliminação segura quando queremos reutilizar um suporte:

- que já contenha dados corporativos;
- que não funciona corretamente;
- ou desfazer-nos de um suporte quando fica obsoleto.

No caso da informação que estiver em suportes não eletrónicos (papel, negativos fotográficos, radiografias, fitas magnéticas, etc.) é necessário utilizar a destruidora para eliminar esta informação. Caso contrário, esta poderia chegar às mãos de terceiros e ser utilizada de forma prejudicial para a empresa.

Por outro lado, se vamos contratar a terceiros a destruição dos nossos dados ou dos suportes, devemos escolher a destruição certificada caso se trate de (ou inclua) dados pessoais ou confidenciais.

**L. POLÍTICA DE CONTROLO DE ACESSOS**

Controlar quem acede à informação da nossa empresa é o primeiro passo para a proteger. É essencial que possamos decidir quem tem permissões para aceder à nossa informação, como, quando e com que finalidade.

Na altura de gerir o controlo de acesso aos nossos dados devemos ter em conta que a informação, os serviços e as aplicações utilizadas não têm por que estar localizados de forma centralizada nas nossas instalações, podem estar distribuídos em equipamentos e redes remotas próprias ou de terceiros. Temos também de considerar que é cada vez mais frequente o uso de dispositivos móveis nos locais de trabalho. Por vezes, estes dispositivos são propriedade do próprio funcionário o que dificulta a tarefa.

Por outro lado, o registo dos acessos em logs dos sistemas será determinante para analisar os incidentes de segurança.

O objetivo é estabelecer quem, como e quando se pode aceder aos ativos de informação da empresa e registar, adequadamente, os referidos acessos.

## PONTOS-CHAVE DA POLÍTICA DE CONTROLO DE ACESSOS

**Política de utilizadores e de grupos** - Definir uma série de grupos que terão determinados acessos para cada tipo de informação estabelecida. Esta classificação pode ser efetuada tendo em conta os seguintes aspetos:

- em função da área ou departamento ao qual o funcionário pertença; em
- função do tipo de informação a que aceda;
- em função das operações permitidas sobre a informação a que se tem acesso.

Em função dos critérios anteriores, podemos estabelecer diversos perfis de utilizador.

**Atribuição de permissões** - Uma vez estabelecidos os tipos de informação, os perfis de utilizadores e os grupos existentes, poderemos concretizar os tipos de acesso à informação aos quais têm direito. As permissões indicarão concretamente quais as ações que podem ser efetuadas sobre a informação (criação, leitura, eliminação, alteração, cópia, execução, etc.). Como norma geral, na definição de permissões, atribuir-se-á o privilégio mínimo.

**Criação/modificação/eliminação de contas de utilizador** - Para permitir o acesso real aos sistemas de informação da empresa devemos ter um procedimento que permita gerir a criação/modificação/eliminação das contas de acesso dos utilizadores (por exemplo: conta de correio, acesso ao CRM, etc.) indicando quem o deve autorizar. Indicaremos detalhadamente os dados identificativos das mesmas, as ações que são permitidas e dotá-las-emos das credenciais de acesso correspondentes que deverão ser fornecidas de forma confidencial aos respetivos proprietários. Serão também incluídos os parâmetros, tais como a caducidade das palavras-passe e os procedimentos de bloqueio oportunos. Deve informar-se o utilizador sobre estes requisitos ao entregar as credenciais, bem como sobre a política de palavras-passe.

**Contas de administrador** - As contas de administrador permitem efetuar qualquer ação sobre os sistemas que administram, pelo que devem ser geridas com a máxima precaução.

**Mecanismos de autenticação** - Definir e implementar os mecanismos de autenticação mais adequados para permitir o acesso à informação da nossa empresa. Teremos em conta aspetos, tais como:

- utilizar mecanismos de autenticação internos ou baseados em serviços de autenticação de terceiros;
- as tecnologias que utilizaremos;
- fatores dos mecanismos de autenticação (um ou vários).

**Registo de eventos** - Estabelecer os mecanismos necessários para registar todos os eventos relevantes no manuseamento da informação da empresa. Registar convenientemente quem acede à informação, quando, como e com que finalidade.

**Revisão de permissões** - Fazer, periodicamente, a revisão das permissões concedidas aos utilizadores para garantir que são adequadas.

**Revogação de permissões e eliminação de contas** - Ao terminar a relação contratual com o funcionário é necessário revogar as suas permissões de acesso aos sistemas de instalações. Eliminar as contas de correio, contas de acesso aos repositórios, serviços e aplicações. Além disso, exigir a devolução de qualquer ativo de informação que lhe tivesse sido atribuído (cartões de acesso ou de crédito, equipamentos, dispositivos de armazenamento, tokens criptográficos, etc.).

## **M. POLÍTICA DE RESPOSTA A INCIDENTES**

É um facto que, apesar das medidas que implementarmos, existe sempre o risco de que ocorra um incidente de cibersegurança. Assim, devemos elaborar um plano de ação que nos indique como atuar da forma mais eficaz possível nestes casos.

Existem muitos tipos de incidentes de cibersegurança, alguns são mais habituais do que outros e enquadram-se numa das seguintes tipologias:

- incidentes não intencionais ou involuntários; danos físicos;
- incumprimento ou violação de requisitos e regulamentos legais; falhas nas configurações;
- recusa de serviço;
- acesso não autorizado, espionagem e roubo de informação;
- eliminação ou perda de informação;
- infeção por código malicioso.

Para executar corretamente o plano e evitar que o dano se estenda, devem ser indicadas detalhadamente as ações a realizar em cada momento, a lista das pessoas envolvidas e as suas responsabilidades, os canais de comunicação oportunos, etc.

Após um incidente, se tivermos aplicado o plano, teremos informação valiosa para conhecer e avaliar os riscos existentes e assim evitar incidentes similares no futuro.

No caso de ocorrerem incidentes graves ou desastres que paralise a nossa atividade principal, aplicaremos o plano de contingência e de continuidade do negócio.

O objetivo é certificarmos-nos de que todos os membros da organização conhecem e aplicam um procedimento rápido e eficaz para atuar perante qualquer incidente em matéria de segurança da informação. Este procedimento incluirá medidas para comunicar de forma correta os incidentes a que correspondam, tanto dentro, como fora da empresa. Incluirá também os mecanismos para registar os incidentes com as suas provas e evidências com o objetivo de estudar a sua origem e evitar que se repitam no futuro.

NUM	MEDIDAS	ENTENDO
M1	Equipa responsável: existe uma equipa responsável que ficará encarregue de gerir os incidentes de segurança.	
M2	Melhoria contínua: é importante disponibilizar toda a informação possível perante os incidentes com o objetivo de os documentar e de garantir uma melhoria contínua.	
M3	Deteção do incidente: qualquer incidente deve ser, imediatamente, comunicado ao pessoal responsável assim que for detetado.	

M4	Avaliação do incidente: a equipa responsável pela gestão do incidente categorizará convenientemente o incidente e atribuirá a classificação da criticidade correspondente.	
M5	Notificação de incidentes: o procedimento para a notificação de um incidente é direto, isto é, a comunicação é feita ao responsável pela gestão dos incidentes.	
M6	Resolução de incidente: a equipa de gestão de incidentes desenvolverá procedimentos de atuação detalhados para dar resposta a cada tipologia de incidente de segurança.	
M7	Tratamento do registo do incidente: deve efetuar-se um registo adequado de toda a informação relativa à gestão do incidente.	

## PONTOS-CHAVE DA POLÍTICA DE RESPOSTA A INCIDENTES

**Equipa responsável** - Para garantir uma resposta eficaz durante o tratamento de incidentes de cibersegurança, deve nomear-se uma equipa responsável pela sua gestão. Teremos de considerar não só o pessoal técnico encarregue da sua resolução (interno ou externo), como também pessoal da direção que deva ser informado permanentemente do estado do incidente.

**Melhoria contínua** - É conveniente analisar a utilidade de usar a informação recolhida na gestão dos incidentes para medir e avaliar a possibilidade de modificar os procedimentos ou acrescentar novas melhorias ou controlos para limitar danos futuros. Podemos executar ações preventivas com o objetivo de dar formação à equipa perante o aparecimento de um possível incidente.

**Deteção do incidente** - Devemos especificar concretamente as situações que são consideradas incidentes.

**Avaliação do incidente** - Uma vez detetado o incidente, devemos categorizá-lo convenientemente e estabelecer a gravidade e a prioridade no seu tratamento.

**Notificação do incidente** - Procurar estabelecer um ponto de contacto único através do qual os funcionários devem notificar os possíveis incidentes ou pontos fracos detetados. De igual modo, deve indicar-se a informação a reunir e as ações imediatas a seguir no momento da notificação.

**Resolução de incidentes** - Desenvolver e documentar procedimentos de resposta para cada um dos tipos de incidentes previamente definidos, dando especial destaque àqueles incidentes mais habituais e perigosos. Serão indicados, detalhadamente, pelo menos os procedimentos para as seguintes ações.

- recolha de evidências assim que for possível após o surgimento do incidente, com o cuidado de manter a cadeia de custódia, a integridade das evidências (codificando-as, se necessário), suportes, etc.;
- estimativa do tempo de resolução;
- realização de uma análise de acordo com os pressupostos requeridos;
- comunicação adequada do incidente no caso de não poder ser resolvido;
- execução de ações concretas para tentar reparar, mitigar ou limitar os danos provocados pelo incidente.

**Tratamento do registo do incidente** - Para dispor de toda a informação sobre o incidente será convenientemente registada, armazenada, entre outra, a informação relativa a:

- data e hora do surgimento do incidente; tipologia e gravidade do mesmo;
- recursos afetados;
- possíveis causas;



## N. POLÍTICA DE CÓPIAS DE SEGURANÇA

Os meios de armazenamento incluem um dos nossos ativos mais valiosos: a informação. Estes dispositivos podem estar envolvidos em situações como roubos, incêndios, inundações, falhas elétricas, avaria ou falha do dispositivo, vírus, eliminações acidentais, etc. Nestes casos, ser-nos-ia impossível aceder à nossa informação, podendo mesmo a continuidade do nosso negócio ficar em risco.

A empresa deve efetuar um inventário de ativos de informação e uma classificação dos mesmos com base na sua criticidade para o negócio. O objetivo desta classificação é ter um registo de todo o software e dos dados imprescindíveis para a empresa para que sirva para determinar a periodicidade dos backups e do seu conteúdo.

A empresa identificará os responsáveis pela realização dos backups e pela definição do procedimento para realização das cópias de segurança e o seu restauro, que incluirá:

- do que se deve fazer; cópia, o tipo de cópia;
- o programa necessário;
- os suportes;
- a periodicidade;
- o prazo de vigência;
- a sua localização;
- e as provas de restauro.

De igual modo, será efetuado um controlo dos suportes utilizados, verificar-se-á que apenas o pessoal autorizado tem acesso e que os suportes são destruídos de forma segura, no caso de terem de ser descartados. Os mesmos critérios de segurança serão aplicáveis no caso de se fazer cópias na cloud ou em fornecedores externos.

O objetivo é verificar que são efetuadas cópias de segurança que garantam a continuidade do negócio.

NUM	MEDIDA	ENTENDO
N1	Inventários de ativos de informação: manter-se-á um inventário atualizado dos ativos de informação (software, dados, suportes, responsáveis, localização, etc.) e serão classificados para identificar os necessários (críticos) para retomar o negócio em caso de desastre ou incidente grave.	
N2	Controlo de acesso: controlar-se-á o acesso às cópias de segurança (apenas pessoal autorizado)	
N3	Cópias de segurança da informação crítica: serão efetuadas cópias de segurança da informação crítica corporativa, da exigida por lei e da estabelecida nos contratos.	
N4	Periodicidade das cópias de segurança: serão efetuadas cópias de segurança.	
N5	Tipo de cópia apropriada: as cópias de segurança deverão ser completas.	
N6	Localização das cópias de segurança: Dever-se-á dispor de, pelo menos, uma cópia completa fora das instalações da organização.	

N7	Cópias na cloud: Serão efetuadas cópias de segurança na cloud. (Caso se aplique) Devem ser tomadas as medidas de segurança necessárias (assinar acordo de encomenda do tratamento com o fornecedor, codificar as cópias, verificar a confidencialidade dos canais de transmissão),	
N8	Procedimentos de cópia e restauro: Elaboram-se e aplicam-se procedimentos de cópia e restauro, revendo-os anualmente e em cada alteração importante nos ativos de informação.	
N9	Verificação de que as cópias foram bem efetuadas: Trimestralmente deve verificar-se a fiabilidade das cópias verificando se é possível restaurá-las.	
N10	Suporte das cópias de segurança: Devem estar etiquetadas e ter um registo dos suportes sobre os quais foi efetuada uma determinada cópia.	
N11	Destruição de suportes de cópia: Quando os suportes utilizados para cópias de segurança são descartados devem ser destruídos de forma segura.	
N12	Codificação das cópias de segurança: Devem ser codificadas as cópias de segurança que contenham informação confidencial ou sensível e a que é carregada para a cloud.	

## *PONTOS-CHAVE DA POLÍTICA DE CÓPIAS DE CÓPIAS DE SEGURANÇA*

**Inventários de ativos de informação** - Deve-se identificar toda a informação necessária para retomar o negócio em caso de desastre ou de incidente grave. Incluir-se-á o software necessário e os dados críticos, os dispositivos que o albergam, os responsáveis, a localização, etc.

**Controlo de acesso** - As cópias de segurança devem ser submetidas a um controlo de acesso restrito ao pessoal autorizado.

**Cópias de segurança da informação crítica** - Teremos de verificar que fazemos cópia de segurança da informação crítica corporativa, da exigida pela lei (por exemplo pelo RGPD) e da estabelecida nos contratos com terceiros.

**Periodicidade das cópias de segurança** - Definiremos com que frequência se devem fazer as cópias de segurança tendo em conta:

- ✓ a variação dos dados gerados;
- ✓ o custo de armazenamento;
- ✓ as obrigações legais.

**Caducidade das cópias de segurança** - Também devemos decidir quanto tempo conservar as cópias em função:

- ✓ de se a informação armazenada continua em vigor;
- ✓ da duração do suporte no qual são efetuadas as cópias;
- ✓ da necessidade de conservar várias cópias anteriores à última realizada.

**Localização das cópias de segurança** - É necessário procurar um lugar adequado para guardar as cópias, com os seguintes critérios:

- ✓ contar com, pelo menos, uma cópia fora da organização;
- ✓ não guardar backups com dados de carácter pessoal (dados de clientes ou de funcionários, por exemplo) em casa;
- ✓ considerar a contratação de serviços de guarda e custódia de acordo com os dados que contêm.

**Cópias na cloud** - Se decidir efetuar a sua cópia na cloud, tome as seguintes precauções para garantir a segurança da informação:

- ✓ codifique a informação confidencial antes de efetuar a cópia;
- ✓ celebre Acordos de Nível de Serviços com o fornecedor, que garantam a disponibilidade, a integridade, a confidencialidade e o controlo de acesso às cópias;
- ✓ considere a largura de banda de que precisa para carregar e descarregar as cópias.

**Procedimentos de cópia e restauro** - Devem ser elaborados e aplicados procedimentos que descrevam como fazer as cópias e como restaurá-las. Desta forma, minimiza-se o tempo necessário para a recuperação dos dados no caso de ser necessário um restauro. Devem ser revistos anualmente e em cada alteração importante do inventário de ativos de informação.

Verificar que as cópias estão bem efetuadas e que é possível restaurá-las. Definir uma periodicidade para efetuar as provas de restauro para garantir que a informação necessária para a continuidade do negócio pode ser recuperada em caso de desastre.

**Suporte das cópias de segurança** - Decidir onde fazer as cópias, tendo em conta os seguintes aspetos:

- ✓ custo, fiabilidade, taxa de transferência e capacidade dos diferentes suportes: discos rígidos externos, USB, bandas, DVD e a cloud;
- ✓ suportes que não estejam obsoletos ou em mau estado.

**Controlo dos suportes de cópia** - Etiquetar e identificar os suportes nos quais são efetuadas as cópias de segurança para que seja possível efetuar um registo dos suportes sobre os quais foi efetuada uma cópia. Assim, no caso de ser necessário recuperar uma informação concreta, agilizaremos o processo ao poder consultar facilmente em que suporte o mesmo foi armazenado.

**Destruição de suportes de cópia** - Quando os suportes utilizados para as cópias de segurança são descartados devemos destruí-los de forma segura. É muito importante garantir que esta informação nunca voltará a estar acessível para evitar possíveis acessos mal-intencionados.

**Codificação da informação** - Codificaremos a informação confidencial e a que requeira armazenamento na cloud, (caso se aplique). Desta forma, protegemos os dados em caso de roubo de informação ou de acessos não autorizado.