# MANUAL DE BOAS PRÁTICAS NA GESTÃO DE INFORMAÇÃO CONFIDENCIAL

ACELERAR O NORTE

# Ficha Técnica

**Título**: Manual de Boas Práticas na Gestão de Informação Confidencial do Projeto Acelerar o Norte

**Conteúdo:** Komodo Consulting

**Revisão:** Acelerar o Norte

**Sumário**: O presente documento apresenta um conjunto de recomendações na gestão de informação confidencial, baseado naquilo que são as melhores práticas sobre o tema. Ainda, as recomendações apresentadas pretendem ajustar-se à realidade do Projeto Acelerar o Norte e às especificidades e desafios inerentes ao conjunto alargado de intervenientes.

**1.ª Edição,** versão 5.0: dezembro de 2024



ACELERAR O NORTE é uma iniciativa dirigida às micro, pequenas e médias empresas das 8 sub-regiões do Norte do país dos setores do comércio, dos serviços pessoais e da restauração e similares, desenvolvido em Consórcio liderado pela Confederação do Comércio e Serviços de Portugal (CCP) e copromovido pela Associação Empresarial de Portugal (AEP), pela Associação da Hotelaria, Restauração e Similares de Portugal (AHRESP) e pela Associação da Economia Digital (ACEPI).

A iniciativa é financiada pela União Europeia através do Plano de Recuperação e Resiliência (PRR) e NextGeneration EU, no âmbito da medida Aceleradoras de Comércio Digital.

# Preâmbulo

A informação é um dos maiores recursos de qualquer organização, já que suporta a maior parte dos processos, como negociações com clientes e fornecedores, tomada de decisões, relacionamento com clientes, dados históricos e de vendas, entre muitos outros.

Os tipos de informação aos quais os colaboradores de uma entidade têm acesso podem ser bastante diferentes, nomeadamente pelo teor dos conteúdos e consequentemente pela classificação de privacidade que se dá aos mesmos.

A informação cujo conteúdo é sensível, privado, ou revela informações que podem colocar em risco o negócio e/ou a reputação das entidades envolvidas, requer tratamento especial e a manutenção e salvaguarda da sua privacidade deve seguir um conjunto de práticas e procedimentos que dificultem ou impossibilitem a divulgação ou perda da mesma.

O projeto Acelerar o Norte apresenta metas ambiciosas, com o objetivo de apoiar mais de oito mil empresas na região Norte. A colaboração e intervenção num número tão significativo de empresas implica, também, que as mesmas partilhem e disponibilizem informação sobre a sua atividade com os membros do projeto.

Essa informação será, muitas das vezes, de caráter sensível, expondo dados da empresa que a mesma preferiria não divulgar, e cuja divulgação pode comprometer a reputação da empresa, a sua potencial vantagem perante a concorrência, entre outros.

Ainda, para atingir este patamar de intervenção, o projeto conta com o trabalho desenvolvido pelos técnicos das estruturas de apoio, denominadas Aceleradoras, que se estabelecem em associações empresariais/locais parceiras do consórcio.

Todas estas especificidades tornam o projeto Acelerar o Norte um projeto com um elevado grau de risco no que diz respeito à gestão de informação confidencial, dada a quantidade de agentes envolvidos, fisicamente estabelecidos em diferentes localizações; dado o volume considerável de dados das empresas com que todos estes intervenientes entrarão em contacto e dado o número de entidades que conformam a gestão do projeto e que devem, por sua vez, assegurar a salvaguarda de informação e a partilha de todos os procedimentos definidos com as equipas envolvidas.

Decorrente da necessidade de garantir a segurança e tratamento apropriado da informação confidencial, foram identificadas um conjunto de boas práticas na gestão de informação confidencial, que pretendem estabelecer algumas recomendações para os procedimentos que devem ser implementados centralmente pelo projeto Acelerar o Norte.

# Informação confidencial

Entende-se por informação confidencial todos os documentos ou informações cujo conhecimento por pessoas não autorizadas é suscetível de colocar em risco os interesses de uma organização ou de lhe causar danos.

Ainda, a informação confidencial inclui aquela que seja partilhada por terceiros com os membros da organização, exclusivamente para a execução das suas atividades, não podendo ser partilhada com outros, e cujo teor não seja de conhecimento público, pelo que a divulgação da mesma compromete a entidade que a partilhou.

A informação classificada como confidencial deve ter acesso condicionado e a divulgação deve ser restrita no seio da organização.

**Boas práticas na classificação de informação confidencial**

Em primeiro lugar, torna-se relevante perceber quando e como é que a documentação deve ser classificada como confidencial.

A informação, de um modo geral, pode ser de procedência interna ou externa.

Interna: contempla os documentos elaborados por membros do projeto Acelerar o Norte, ou por entidades externas que, contratualmente, se encontrem ao serviço do projeto.

Externa: documentos elaborados por entidades externas ao projeto e partilhados com algum dos membros do projeto.

Para além da classificação referente à sua procedência, a informação pode ser catalogada de acordo com o seu grau de sensibilidade, permitindo identificar conjuntos de dados que não devem ser conhecidos fora da organização ou mesmo dentro de certas partes da mesma.

Para atribuir uma classificação segundo o grau de sensibilidade é importante fazer um levantamento do tipo de informações, aplicações e respetivos detalhes, fazendo uma correspondência entre aplicações informáticas e subdomínios de dados, podendo chegar a uma classificação, por exemplo de:

- Informação pública: não existem restrições à partilha de informação;
- Informação interna: a informação está disponível para todos os colaboradores da organização;
- Informação restrita: informação sujeita a condições de acesso;
- Informação confidencial: informação apenas acessível a utilizadores com direito explícito de acesso.

**O presente Manual de Boas Práticas incide na Gestão de Informação classificada como confidencial.**

Qualquer documento que tenha sido desenvolvido pelos membros do projeto Acelerar o Norte que não se pretenda divulgar ou que não tenha sido criado com a expressa intenção de ser partilhado, deve ser considerado como confidencial e identificado como tal.

No momento de criação/elaboração de um documento interno, a classificação é efetuada mediante a inclusão no documento da menção "Confidencial".[1]

No caso de documentos externos, quando se trata de documentação produzida por outras entidades, ela deve estar classificada como confidencial para que seja considerada como tal. Aquando da receção de um documento, o mesmo já poderá ter sido classificado pela entidade externa ou carecer de classificação, que é atribuída após a análise do conteúdo.

Ainda, na interação com beneficiários, parceiros e outros *stakeholders* poderá haver partilha, em suporte escrito ou não, de informação confidencial relativa ao negócio dos mesmos, como por exemplo: nomes de clientes, planos de marketing, estratégias de venda, planos de desenvolvimento de produtos, dados financeiros, entre outros.

Quando se realiza alguma recolha de dados em que se necessita da identificação de um indivíduo, esta informação deve ser considerada como confidencial e encontra-se ao abrigo do Regime Geral de Proteção de Dados, devendo ser respeitadas as disposições nele presentes.

## Políticas e Gestão

### Controlo de acessos

A informação confidencial deve ser de acesso restrito, de forma que seja protegido o seu conteúdo, que não existam acessos não autorizados ou alterações, e que apenas quem necessita da informação para a execução das suas atividades tenha acesso à mesma.

O controlo de acessos é um elemento fundamental de segurança que determina quem tem autorização para aceder a determinados dados, aplicações e recursos e em que circunstâncias. Tal como em um espaço físico, as chaves, as listas de participantes e os cartões de acesso protegem o dito espaço, os controlos de acesso protegem os espaços digitais.

As políticas de controlo de acessos dependem fortemente de técnicas como autenticação e autorização, permitindo que as organizações verifiquem explicitamente a identidade dos utilizadores e se os mesmos têm o nível de acesso necessário para o desenvolvimento das suas funções.

O objetivo do controlo de acessos é impedir que as informações confidenciais cheguem às mãos de agentes maliciosos. Os ciberataques a dados confidenciais podem ter consequências graves, como perda de propriedade

[1] É possível acrescentar, nos programas Office uma indicação de confidencialidade através da ferramenta Marca de Água, disponível no separador Estrutura.

intelectual, divulgação de segredos de negócio, exposição de informações pessoais e de clientes, entre outros.

Atualmente, o controlo de acessos é uma componente essencial da estratégia de segurança, sendo também uma das melhores ferramentas para minimizar o risco de segurança do acesso não autorizado aos respetivos dados.

Na sua forma mais simples, o controlo de acessos envolve a identificação de um utilizador com base nas respetivas credenciais, e em seguida a autorização do nível de acesso de informação pretendido, após autenticação.

**Melhores práticas a considerar:**

1. **Definição de uma política de controlo de acessos:** tendo por base ferramentas de controlo de acesso, é essencial definir um conjunto de diretrizes para regular e gerir o acesso a informação e a forma como são atribuídos os acessos às pessoas conforme a necessidade decorrente das suas funções e atividades (a quem, ao que, quando e como).

2. **Palavras-passe:** a proteção por palavra-passe é uma das ferramentas de segurança de dados mais comuns e elementares disponíveis para utilizadores. Devem ser acionadas, mas, para que não sejam facilmente contornadas por *hackers*, devem ser garantidos alguns critérios na sua criação:

   Diretrizes para a criação de uma palavra-passe segura:

   - Extensão de, pelo menos, 12 caracteres;
   - Combinação de letras, números e símbolos;
   - Utilização de, pelo menos, uma letra maiúscula;
   - Palavras invulgares e não relacionadas com informações pessoais.

   As palavras-passe são a primeira linha de defesa contra o acesso ilícito a contas, dispositivos e ficheiros online. Quanto mais forte, maior a proteção que confere.

   Comportamentos que aumentam a proteção contra *hackers*

   - Utilização de palavras-passe fortes em todos os dispositivos;
   - Alteração de palavras-passe com regularidade;
   - Não abrir ligações e anexos suspeitos ou de procedência desconhecida;
   - Proteger a exposição do computador, ecrãs e teclados, impedindo que terceiros possam visualizar ou perceber as palavras que estão a ser digitadas;
   - Evitar o acesso a dados pessoais e financeiros através de redes públicas;
   - Softwares de antivírus e antimalware em todos os dispositivos.

### Como é que as palavras-passe são acedidas de modo ilícito?

Os agentes maliciosos utilizam uma variedade de táticas para roubar palavras-passe, incluindo:

- **Ataques de força bruta**: um método que utiliza tentativa e erro para descodificar palavras-passe e credenciais de início de sessão de modo a obter acesso ilícito a contas e sistemas.
- **Ataques de *credential-stuffing***: a utilização automática de nomes de utilizador e palavras-passe roubados para obter acesso ilícito a contas online.
- **Ataques de dicionário**: os hackers tentam descodificar a palavra-passe ao introduzir cada palavra do dicionário, através de derivados dessas palavras com alteração de carateres e carateres alfanuméricos e através de palavras-passe e expressões-chave que foram alvo de fuga de dados.
- ***Keylogging***: utilização de um programa de software para controlar os toques no teclado de um utilizador para roubar PIN, números de cartões de crédito, nomes de utilizador, palavras-passe e muito mais.
- ***Malware*:** software malicioso concebido para prejudicar ou explorar sistemas informáticos e, em muitos casos, roubar palavras-passe.
- **Utilização de palavra-passe única**: o uso de uma única palavra-passe em várias contas de modo a evitar bloqueios de contas e manter-se indetetável.
- ***Phishing***: os utilizadores são levados a partilharem as respetivas credenciais com *hackers*, que se fazem passar por instituições e fornecedores legítimos.

Fonte: Microsoft Security

## 3. Autenticação multifator

A autenticação multifator é um fator de segurança adicional que obriga os utilizadores a apresentar duas ou mais formas de identificação para autenticação. Como método de controlo de acessos, melhora significativamente a segurança ao adicionar várias camadas de defesa e reduzindo, consequentemente, a probabilidade de acessos não autorizados.

Os fatores de autenticação, por norma, incluem duas das seguintes categorias:

1. Algo que se sabe: refere-se à informação que é sabida pelo utilizador como palavras-passe, PINs, ou respostas a perguntas de segurança.

2. Algo que se possui: refere-se a objetos físicos que o utilizador detém, como *smartphones*.
3. Algo que se é: relaciona-se com fatores indissociáveis da pessoa, como impressões digitais, reconhecimento facial, entre outros.

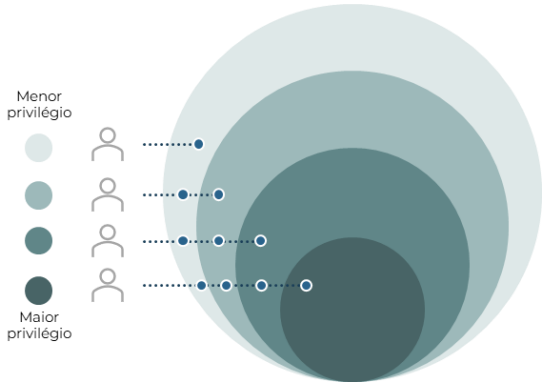
   A autenticação multifator garante que, na eventualidade de um dos meios estar comprometido, o acesso não autorizado continua a ser pouco provável.

4. **Princípio do menor privilégio:** um utilizador deve ter acesso apenas ao que é absolutamente necessário para desempenhar as suas funções.

   Ao minimizar as permissões, limitam-se os danos que podem ser causados por uma conta comprometida ou por uma ameaça interna.

   A maior parte das organizações não permite o acesso administrativo aos computadores dos utilizadores, visto que isto não é essencial para a execução das funções, necessitando de aprovações quando se pretende fazer alguma instalação ou alteração. Do mesmo modo, diferentes áreas funcionais não necessitam de acesso a informações de outras áreas para o desenvolvimento da sua atividade.

   Para implementar uma política de menor privilégio devem ser definidas as funções e os acessos que cada utilizador necessita, restringir os acessos em consonância e garantir que periodicamente são revistas as funções e permissões atribuídas.




5. **Controlos de acesso baseados em *roles* (RBAC[2])**

   Tendo definido que é necessário diferenciar o tipo de acessos à informação que cada utilizador tem, assim como o que pode realizar - visualizar, editar, modificar, eliminar documentos - torna-se necessário criar e atribuir essas permissões.

   O controlo de acesso baseado em *roles* permite que, em vez de se efetuar uma atribuição de permissões individualizada a cada utilizador, sejam atribuídas diferentes permissões a *roles* específicos, e depois sejam

[2] *Role-based access control*

atribuídos *roles* a cada utilizador. Assim, o processo é simplificado e as alterações que possam vir a ser efetuadas são realizadas de forma transversal ao *role* e não ao indivíduo.

Um *role* pode representar um descritivo de funções, um nível de responsabilidade, ou um cargo. Este método também prevê que exista uma hierarquia de roles, permitindo que níveis hierárquicos superiores automaticamente herdem as permissões de níveis inferiores acrescidas de outras relevantes para a função.

**Política de retenção de dados**

Uma política/procedimento de retenção de dados estabelece e descreve a forma como se espera que a organização gira informação, desde a sua criação ou receção até à sua destruição.

De uma forma geral, a informação confidencial referente a terceiros apenas é armazenada durante o tempo em que se necessite da mesma para a execução das atividades. Finda a necessidade, a informação deve ser eliminada. Contudo, há situações em que a lei prevê o armazenamento de dados durante períodos superiores de tempo.

O período de tempo durante o qual os dados pessoais são armazenados e conservados varia de acordo com a finalidade para a qual a informação é tratada. Efetivamente, existem requisitos legais que obrigam a conservar os dados por um período de tempo mínimo. Assim, e sempre que não exista uma exigência legal específica, os dados serão armazenados e conservados apenas pelo período mínimo necessário para a prossecução das finalidades que motivaram a sua recolha ou o seu posterior tratamento, nos termos definidos na lei.

**Acordos de confidencialidade**

Um acordo de confidencialidade é um acordo formal entre duas ou mais partes, que pretendem partilhar informação relevante entre si, mas em que devem garantir que a mesma não seja divulgada com terceiros, pelo que se comprometem a não divulgar as informações protegidas pelo acordo.

Este acordo obriga as partes envolvidas a manter sigilo sobre todas as informações confidenciais a que possam ter acesso, e deve ser redigido por um advogado para garantir a sua validade legal.

Um acordo de confidencialidade pode ser celebrado entre qualquer pessoa, singular ou coletiva, pública ou privada, ou inclusive com os colaboradores de uma empresa.

## Infraestrutura

A crescente dependência em sistemas interconectados e redes leva a que a segurança em termos de infraestrutura digital seja um dos aspetos mais relevantes das operações modernas. Em qualquer tipo de organização, a

proteção e segurança da infraestrutura de rede é imperativa para garantir a continuidade do negócio e a defesa perante potenciais ameaças.

**Antivírus e antimalware, Firewall e Sistema de deteção de intrusos**

As soluções de antivírus e antimalware são cruciais para a gestão de informação confidencial dado que fornecem proteção essencial contra várias formas de *malware* como vírus, *ransomware*, *spyware*, *trojans* e outros softwares maliciosos.

Este tipo de softwares maliciosos pode comprometer a confidencialidade de dados sensíveis através do roubo, corrupção ou exposição de informações a terceiros não autorizados. Pelo que através da prevenção de ataques, consequentemente se protege a confidencialidade de informação e a integridade do sistema.

Para além das soluções essenciais de antivírus, no âmbito de uma organização, um dos aspetos mais relevantes a considerar é a existência de *firewalls* que no fundo agem como barreiras entre as redes internas e a internet, controlando o tráfego em ambos os sentidos, baseando-se em algumas regras de segurança pré-definidas.

Um sistema de deteção de intrusos trabalha através da monitorização do tráfego da rede, alertando para ataques e tentativas de intrusão.

Os diferentes tipos de medidas de proteção são complementares e, embora se possam sobrepor em alguns aspetos, de um modo geral têm objetivos diferentes, pelo que devem ser considerados de uma forma holística.

**Encriptação de dados**

A encriptação é o processo de utilização de algoritmos de criptografia para tornar os dados ilegíveis e bloquear os dados com uma "chave". No estado encriptado, os dados não podem ser decifrados, sendo apenas desencriptados através de uma chave emparelhada com a chave de encriptação, pelo que caso a informação seja acedida de forma não autorizada a mesma se mantém ilegível.

As estratégias de encriptação ajudam a prevenir fugas de confidencialidade e adulteração de dados.

Os mecanismos de encriptação de dados precisam de proteger os dados em três fases:

- Dados inativos / armazenados: são todas as informações que são mantidas em objetos de armazenamento;
- Dados em trânsito: são informações transferidas entre componentes, localizações ou programas, sempre que se partilha informação;
- Dados em utilização: são dados que estão a ser trabalhados ativamente na memória.

A encriptação de dados é, atualmente, uma prática frequente e basilar da maioria dos programas padrão utilizados, assim como dos protocolos de comunicação através da internet. As estratégias de encriptação têm um papel crucial na proteção de informação sensível que é partilhada através da internet ou que se encontra armazenada. Não só protege a confidencialidade dos dados como permite autenticar a sua origem, garantir que a informação não foi adulterada após o envio e prevenir práticas de repudiação.

**Canais de comunicação seguros e partilha de dados**

Para além da codificação da informação que é partilhada, é fundamental evitar que a informação seja intercetada por terceiros e assegurar que a transferência entre partes seja efetuada da forma mais segura possível.

Para tal, existem protocolos de transferência segura de dados que são estabelecidos entre as entidades entre as quais se partilha informação, cujo papel é garantir a integridade dos dados, fornecendo meios para salvaguardar a informação e, por conseguinte, mitigando os riscos associados à partilha com terceiros. A implementação destes protocolos, por norma, já faz parte da segurança de softwares, websites, etc.

No que se refere às atividades diárias dos membros do projeto e à forma como partilham informação entre si, e com terceiros (como por exemplo as empresas beneficiárias) podem ser identificadas algumas boas práticas, como sejam:

- Evitar partilhar conteúdos do projeto, confidenciais ou com informação sensível através de canais não seguros como WhatsApp, Messenger, sms, ou outros serviços de mensagens pessoais e informais.
- Partilhar conteúdos através da plataforma definida para o projeto, evitando que haja comunicações fora da mesma.
- Caso haja necessidade de partilhar links de acesso a informação com terceiros, deve-se garantir que são definidas as permissões de acesso dos utilizadores que recebem o link e que o mesmo tem uma data de validade, a partir da qual não é possível aceder aos conteúdos.
- Estabelecimento de canais de comunicação e/ou permissões específicas para a partilha de informação dentro da organização, como por exemplo através de canais de Teams ou de pastas partilhadas (OneDrive ou semelhantes).

**Mascaramento de dados e anonimização**

A anonimização de dados diz respeito à técnica de processamento de dados que remove ou modifica informações que possam identificar uma pessoa ou entidade. O processo resulta em dados anonimizados que não podem ser associados a nenhum indivíduo ou entidade específica.

Para além da proteção que permite contra violações de dados, já que os torna inúteis caso sejam obtidos, a anonimização ajuda as organizações a cumprir

leis e regulamentos sobre privacidade de dados, como aquelas que são estabelecidas no Regime Geral de Proteção de Dados (RGPD).

Existem diversas técnicas, dependendo da natureza dos dados e do grau de usabilidade que se pretende posteriormente.

- **Encobrimento de caracteres:** consiste em ocultar, ou tornar ilegíveis, partes de um documento. É utilizada, por exemplo, para ocultar números de contas bancárias ou cartões de crédito.
- **Pseudonimização**: envolve a substituição de campos de identificação por informação artificial ou pseudónimos.
- **Generalização:** redução da granularidade dos dados, por exemplo substituindo idades exatas por intervalos ou localizações exatas por concelhos ou regiões.
- **Embaralhamento**: consiste em movimentar ou baralhar a informação dentro de um mesmo campo, de forma que se preserve a distribuição ou a informação estatística, enquanto se afastam os valores individuais ou específicos do seu registo original.
- **Geração de dados**: envolve a criação de um conjunto de dados novos, artificiais e diferentes do conjunto de dados original, que preserva as propriedades estatísticas, mas que não contém qualquer informação confidencial.

**Backup e prevenção de perda de dados**

O backup de dados consiste na realização de cópias de segurança, de uma localização primária a uma localização secundária, de forma a proteger a informação em caso de acidentes ou ações maliciosas, permitindo também a continuidade do negócio e a retoma de atividades.

Existem várias opções para o armazenamento de cópias de segurança, entre as quais:

- Dispositivos físicos removíveis como discos rígidos externos, CDs, DVDs, pendrives. A sua portabilidade e custo reduzido tornam-nas uma opção popular, contudo estão limitadas em termos de capacidade e são suscetíveis a danos provenientes do ambiente em que se encontram (humidade, calor, etc.), podendo também ser alvo de furto.
- Redundância: envolve a criação de múltiplas cópias dos dados, em diferentes plataformas, e pode ser alcançada através da utilização de múltiplos discos rígidos, ou da utilização de serviços de backup em *cloud*.

Independentemente da estratégia, uma das componentes essenciais é a existência de um software de backup que garanta a recuperação rápida, segura e eficiente de dados, tendo em consideração que o mesmo deve incluir: automatização e calendarização de cópias de segurança frequentes; capacidade de backup incremental e diferencial, gravando apenas as alterações e poupando tempo e espaço; encriptação de dados; compressão de tamanho de ficheiros e destinos múltiplos de *backup*.

Dentro das boas práticas nas estratégias de *backup*, destaca-se a **estratégia 3-2-1**, que contempla **três cópias da informação** (a original e duas cópias duplicadas), armazenadas em **dois suportes diferentes** (ex: dispositivo removível e armazenamento em cloud), em que **uma das localizações de dados armazenados é externa** ao local da organização.

## Monitorização e registo de atividades

Uma infraestrutura segura inclui a capacidade de rastrear os acessos a informação sensível e monitorizar as atividades dos utilizadores. Ao manter um registo detalhado, as organizações conseguem detetar e investigar qualquer tipo de tentativas não autorizadas de acesso a informação confidencial, contribuindo para a salvaguarda desta informação.

O tipo de informação que se regista deve conter datas e horas de acesso, operações realizadas – como *downloads* - e ficheiros acedidos. Isto permite também que nas situações em que possa ter havido uma fuga de informação, seja possível haver rastreabilidade e uma identificação mais célere dos pontos de fuga, de modo a poderem ser colmatados.

## Política de gestão de riscos

As ameaças no mundo digital são dinâmicas e rapidamente se torna necessário rever as políticas e procedimentos estabelecidos, garantindo que estão em concordância com a vanguarda do setor.

Da mesma maneira, novas formas de trabalhar dentro da organização, novos processos e/ou novos contactos podem criar e expor novas vulnerabilidades, pelo que é essencial que os processos de segurança de informação sejam revistos periodicamente e exista uma cultura de identificação proativa de vulnerabilidades e riscos.

Uma das estratégias mais frequentes utilizadas pelas organizações é a realização de testes de penetração e vulnerabilidade dos sistemas, em que são simulados ataques cibernéticos que ajudam a identificar vulnerabilidades críticas de segurança e reforçar as medidas implementadas.

Tal como é fundamental ter uma postura proativa na identificação de riscos, é crucial a celeridade do restabelecimento da operação caso se verifique a materialização das ameaças, e a isto chama-se habitualmente uma Política de Gestão da Continuidade de Negócio.

Assim, devem estar instituídas políticas e procedimentos que procurem garantir o retorno aos padrões normais de atividade e a recuperação atempada no caso de ocorrência de eventos disruptivos. Os eventos disruptivos podem tomar a forma de catástrofes naturais, pandemias, atos de terrorismo, falhas nos sistemas informáticos, incêndios, inundações ou falhas graves de energia.

Para isso, a implementação de todas as estratégias referidas anteriormente se conjuga no sentido de fornecer essa capacidade de recuperação e posterior aferição, como através da recuperação de dados armazenados de forma segura, os registos de atividade, os relatórios de análises de vulnerabilidade e o registo de acessos.

## Recursos Humanos

As pessoas desempenham um papel fundamental no sucesso de qualquer organização. Num mundo cada vez mais competitivo, o capital humano é determinante para o desenvolvimento de qualquer atividade empresarial.

Diferentes organizações necessitam de diferentes competências por parte dos seus colaboradores, embora, atualmente, muitas das atividades tenham recurso, de uma forma ou outra, a computadores e redes, pelo que se torna crucial que os utilizadores estejam conscientes não só das vantagens como também das vulnerabilidades que um mundo cada vez mais globalizado acarreta.

São também os colaboradores os responsáveis pelo sucesso das suas organizações não só no que diz respeito às atividades que efetuam, mas também no que concerne à capacidade que têm de as proteger, em termos de ameaças e de reputação através dos seus comportamentos.

No que se refere especificamente aos membros do projeto Acelerar o Norte, importa referir que, dada a dimensão e ambição do projeto, os seus membros estarão em contacto frequente com informações sensíveis e potencialmente confidenciais sobre diferentes *stakeholders* nacionais e internacionais, podendo causar danos graves ao negócio ou à reputação dos mesmos e do projeto, caso não estejam conscientes e preparados para gerir essa informação confidencial.

Para além de todas as medidas que possam ser implementadas de uma forma centralizada, e que em muito auxiliam a mitigação de riscos de perda de informação, quebra de confidencialidade e exposição de dados pessoais, entre outros, a conduta dos colaboradores, a sua consciencialização sobre os riscos e o seu conhecimento sobre os procedimentos e regras que devem cumprir é um fator crítico de sucesso para a segurança da informação.

No que se refere aos temas relacionados com colaboradores, destacam-se as seguintes práticas e condutas a reter:

1. **Comportamento preventivo**

   Todos os membros do projeto devem pautar-se por uma postura de prevenção de riscos, estando conscientes das consequências e reportando de imediato qualquer potencial suspeita de concretização dos riscos, ou qualquer situação desconfortável com que se possam encontrar, especialmente naquelas que se referem a e-mails, pedidos de dados, links não identificados, entre outros.

De uma forma geral, a metodologia presente no Código de Ética e Conduta, na secção da tomada de decisões, é extensível ao que se relaciona com dados e informação confidencial, evitando a realização de determinado ato se o mesmo potencialmente: for contra a lei, contra os valores do consórcio e projeto, tiver o potencial de causar danos à reputação do projeto ou de terceiros ou viole alguma obrigação assumida com entidades externas e/ou parceiros.

Ainda, na tomada de decisão ou quando confrontado com situações que possam suscitar dúvidas, pode-se utilizar também outra metodologia mais simples e comum, colocando a pergunta ***"E se?"***, a qual consiste em imaginar todas as ramificações possíveis das potenciais consequências ao executar uma possível ação ou de um determinado evento ocorrer. Por exemplo, "E se eu não cumprir com os procedimentos instalados relativos à partilha de informação de forma segura, a consequência poderá ser quebra de confidencialidade, partilha de informação sensível e, em último caso, dano à reputação e risco de encerramento do projeto?".

Através de uma postura preventiva e cautelosa é possível minimizar a probabilidade de ocorrência dos riscos relacionados com a informação confidencial.

## 2. Formações e capacitações

É importante referir que, na maior parte das situações, os colaboradores das organizações não têm intenção maliciosa, mas criam ameaças à segurança por meio de ignorância ou descuido — por exemplo, cair em um ataque de *phishing*, ignorar os controlos de segurança numa tentativa de poupar tempo, perder um computador que pode ser usado para aceder à rede da organização ou enviar por e-mail os arquivos errados, para indivíduos fora da organização.

As formações ou capacitações são uma das ferramentas mais eficientes para garantir que os membros do projeto estão familiarizados com os procedimentos e políticas definidos.

De uma forma centralizada, o projeto deverá garantir que os procedimentos e formas de atuar que se esperam dos membros do projeto lhes são transmitidos através da realização de sessões presenciais, remotas ou em formato *e-learning* obrigatório.

Ainda, a existência de uma base de dados de consulta, com sessões gravadas ou conteúdos que contenham os principais pontos a reter são identificados como boas práticas, já que permitem que, rapidamente, quando confrontado com situações dúbias, o colaborador possa verificar o comportamento que dele é esperado.

A participação nas sessões e a consulta da informação é um dever dos membros do projeto, necessário e precedente à execução das suas atividades, não podendo alegar em qualquer momento desconhecimento das políticas ou procedimentos definidos pelo projeto.

De realçar que, para o projeto, a inexistência de procedimentos inadequados e uma falta de consciencialização dos membros sobre as práticas de segurança de informação podem-se revelar catastróficas. Dado o teor e o volume de informação com que os membros do projeto terão de lidar, assim como o número de beneficiários com que partilharão informação, a proteção dos dados é essencial para a atividade do projeto, sendo que a capacitação dos membros se torna imperativa para educar e sensibilizar sobre os riscos e medidas de mitigação.

Ainda, os conteúdos formativos devem ser constantemente alvo de revisão e as sessões de formação ou capacitação devem ocorrer com alguma periodicidade, que permita a atualização e reforço de conhecimentos.

### 3. Estabelecimento ou cessação de vínculo laboral

Quando se verifique a necessidade de incorporar um novo elemento no projeto Acelerar o Norte, importa garantir que o mesmo é informado sobre todas as políticas do projeto que concernem a gestão de informação, e que lhe é facilitada toda a informação que permite que o colaborador esteja em capacidade de cumprir com essas diretrizes.

Também no momento de cessação de vínculo laboral, devem ser reforçadas clausulas de confidencialidade que vigorem no âmbito do projeto e devem ser imediatamente eliminados todos os acessos e recolhidos todos os equipamentos que sejam propriedade do projeto, numa tentativa de reduzir a possibilidade de ações maliciosas por parte de colaboradores em cessação de funções.

### 4. Política de uso de dispositivos pessoais

Atualmente, cada indivíduo possui um conjunto de dispositivos que permitem ligações remotas e através dos quais potencialmente conseguirão aceder a plataformas do projeto, por isso é importante clarificar e estabelecer diretrizes para o uso de dispositivos pessoais, como *smartphones* e computadores pessoais ou de familiares, para aceder a informações confidenciais do projeto.

Os membros do projeto Acelerar o Norte devem desenvolver as suas atividades utilizando os dispositivos eletrónicos facultados pelo projeto, evitando ao máximo o acesso a conteúdos do projeto através de outros dispositivos.

Ainda, devem evitar a partilha dos dispositivos facultados pelo projeto com outros, como sejam família, amigos, colegas, que podem colocar em risco a integridade da informação.

### 5. Práticas diárias relacionadas com o local de trabalho

Adicionalmente ao comportamento com os dispositivos digitais, importa ainda pensar nos espaços físicos onde desenvolverão a sua atividade, e a

potencial quebra de confidencialidade que pode advir da existência de informação em físico ou da capacidade de terceiros observarem os conteúdos de trabalho.

Assim, algumas práticas recomendadas assentam em:

- Manter o espaço de trabalho livre de qualquer documento ou suporte de informação que contenha dados pessoais ou sensíveis, informações secretas e/ou confidenciais, sempre que o mesmo seja deixado sem supervisão por um longo período, assim como no final do dia de trabalho;
- Toda a informação que contenha dados pessoais, privados, secretos e confidenciais deverá ser retirada da mesa depois de utilizada e armazenada em local seguro e com controlo de acessos;
- Deve ser reduzida a impressão de documentos e manutenção de cópias físicas, contudo se for necessário, todos os documentos e suportes físicos de informação devem ser guardados em gavetas adequadas com fechaduras e/ou outra forma segura de mobiliário, quando não estiverem a ser utilizados, especialmente fora dos horários de trabalho;
- Os computadores e dispositivos móveis deverão ser bloqueados sempre que o utilizador se ausentar, e desligados no final do dia de trabalho;
- Todas as impressões com informação pessoal, privada, secreta ou confidencial, utilizada ou processada por equipamentos de suporte, por exemplo impressoras, fotocopiadoras e/ou digitalizadores, devem ser retiradas dos mesmos imediatamente após o seu processamento terminar;
- Nenhuma informação de acesso reservado pode ser retirada das instalações designadas como localização principal de trabalho sem expressa autorização de um superior hierárquico;
- Fora das instalações de trabalho designadas como localização principal, os membros do projeto são responsáveis pela salvaguarda do equipamento e da informação a eles confiadas, devendo adotar uma postura de salvaguarda dos equipamentos e dados.

## 6. Responsabilidades individuais

Cada um dos membros do projeto Acelerar o Norte, representa o projeto em cada uma das interações que sustém com outras entidades, pelo que deve existir em cada indivíduo um elevado grau de responsabilidade pela manutenção da reputação do projeto, assim como um elevado zelo pela salvaguarda dos objetivos do mesmo.

Da mesma forma, cada membro do projeto é responsável pela manutenção da segurança e pelo respeito pelos princípios de conduta, devendo ter também um papel de reporte e comunicação de quaisquer

preocupações relacionadas com segurança de informação, para além daquelas já explicitadas no Código de Ética e Conduta.

# Regulamento Geral sobre Proteção de Dados

O cumprimento da legislação relativa à proteção de dados pessoais e ao respeito pelos direitos dos respetivos titulares deve ser uma matéria de maior importância para o projeto Acelerar o Norte.

Os dados pessoais são recolhidos e tratados no estrito respeito e cumprimento do disposto na legislação de proteção de dados pessoais em vigor em cada momento, nomeadamente o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 ("RGPD") e a Lei n.º 58/2019, de 8 de agosto de 2019.

O Regulamento Geral sobre Proteção de Dados Pessoais (RGPD) consagra um conjunto de alterações legislativas importantes no que diz respeito ao reforço dos direitos dos titulares dos dados pessoais e no que diz respeito às medidas que devem ser adotadas pelas empresas e entidades públicas para proteção de dados pessoais.

**Entidade responsável**

O projeto Aceleradoras Norte é uma iniciativa do Consórcio Aceleradoras Norte, constituído pelas seguintes entidades, as quais são conjuntamente responsáveis pelo tratamento dos seus dados pessoais:

- Confederação do Comércio e Serviços de Portugal - https://ccp.pt/;
- AEP - Associação Empresarial de Portugal - https://www.aeportugal.pt/;
- AHRESP - Associação da Hotelaria, Restauração e Similares de Portugal - https://ahresp.com/;
- ACEPI - Associação do Comércio Eletrónico e da Publicidade Interativa - https://www.acepi.pt/.

**Tratamento de dados**

O tratamento de dados pessoais consiste numa operação ou conjunto de operações efetuadas sobre dados pessoais ou conjuntos de dados pessoais, através de meios automatizados, ou não, nomeadamente a recolha, o registo, a organização, a estruturação, a conservação, a adaptação, a recuperação, a consulta, a utilização, a divulgação, difusão, comparação, interconexão, a limitação, o apagamento ou a destruição.

**Tipo de dados pessoais tratados**

Tendo em consideração que a relação que se estabelece entre os membros do projeto e os beneficiários pode ser considerada uma relação *business-to-business*, muitos dos dados recolhidos são considerados públicos, já que dizem respeito a informação genérica da empresa (nome da empresa, número de identificação de pessoa coletiva, sede, entre outros).

Contudo, a empresa é representada por indivíduos, indivíduos esses que poderão vir a partilhar os seus dados pessoas, quando assim for solicitado pelo projeto. Esses dados, como nome, cargo, contacto, assim como os dados que se relacionam com os acessos desses indivíduos à plataforma do projeto,

como *cookies* e outras tecnologias de rastreio carecem de tratamento concordante com o Regulamento Geral sobre Proteção de Dados.

**Medidas adotadas**

O projeto Acelerar o Norte deve implementar medidas técnicas alinhadas com as melhores práticas do mercado e desenvolver processos e procedimentos que permitam manter todos os dados pessoais em condições adequadas de segurança face aos riscos envolvidos.

Estas medidas de segurança visam a proteção dos dados contra a difusão, perda, uso indevido, alteração, tratamento ou acesso não autorizado, bem como contra qualquer forma de tratamento ilícito.

Não obstante as medidas de segurança que sejam adotadas pelo projeto, de caráter técnico e organizativo, as recomendações presentes neste Manual de Boas Práticas de Gestão de Informação Confidencial devem ser consideradas, assegurando, nomeadamente a atualização de dispositivos em termos de configurações de segurança, antivírus e antimalware, e a adoção de um comportamento preventivo na utilização e acesso a informação do projeto.

**Comunicação de dados com terceiros e/ou subcontratados**

O projeto Acelerar o Norte, de forma centralizada, ou qualquer um dos membros do consórcio, de forma individual, no âmbito da sua atividade, poderá recorrer a terceiros para a prestação de determinados serviços.

Por vezes, a prestação destes serviços implica o acesso, por estas entidades, a dados pessoais dos beneficiários. Caso se revele necessária esta partilha, o projeto Acelerar o Norte deve garantir que as entidades que tenham acesso aos dados sejam reputadas e ofereçam as mais elevadas garantias a este nível, o que fica devidamente consagrado e acautelado contratualmente.

Assim, qualquer entidade subcontratada pelo projeto Acelerar o Norte deverá tratar os dados pessoais, em nome e por conta do projeto Acelerar o Norte e adotando as medidas necessárias de forma a proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizado e contra qualquer outra forma de tratamento ilícito.

Em qualquer dos casos, o projeto Acelerar o Norte permanece responsável pelos dados pessoais que lhe sejam disponibilizados.

**Tempo de armazenamento de dados**

O período de tempo durante o qual os dados pessoais são armazenados e conservados varia de acordo com a finalidade para a qual a informação é tratada.

Efetivamente, existem requisitos legais que obrigam a conservar os dados por um período de tempo mínimo. Assim, e sempre que não exista uma exigência legal específica, os dados serão armazenados e conservados apenas pelo período mínimo necessário para a prossecução das finalidades que

motivaram a sua recolha ou o seu posterior tratamento, nos termos definidos na lei.

**Direitos**

Enquanto titulares dos dados pessoais, deve ser garantido aos indivíduos, a qualquer momento, o direito de acesso, retificação, atualização, limitação e eliminação dos seus dados pessoais, o direito de oposição à utilização dos mesmos para fins comerciais pelo projeto Acelerar o Norte e à retirada do consentimento, sem que tal comprometa a licitude do tratamento efetuado ao abrigo desse consentimento, bem como o direito à portabilidade dos dados.

O exercício dos direitos acima descritos poderá ser solicitado, pelo titular dos dados pessoais, diretamente ou mediante pedido por escrito, através dos contactos disponibilizados para o efeito no presente documento, bem como demais contactos disponibilizados pelo Acelerar o Norte.

De uma forma geral, o projeto Acelerar o Norte contempla o envolvimento de um conjunto alargado de intervenientes, de entre os quais os membros do consórcio e respetivas equipas, os membros das Aceleradoras, os beneficiários e os parceiros estratégicos.

O número significativo de pessoas que contactam com diferentes tipos de informação, sendo em grande parte informação confidencial dos beneficiários, representa um desafio para o projeto.

Neste sentido, com base nas boas práticas de gestão de informação confidencial identificadas, são sugeridos um conjunto de aspetos que o projeto deve garantir de forma centralizada e os principais comportamentos e procedimentos que se recomenda pautem a atuação dos membros do projeto.

**Estrutura central do projeto**

- Estabelecer os critérios de classificação de informação confidencial;
- Estabelecer e implementar uma política de controlo de acessos, que contemple a obrigatoriedade de palavras-passe seguras e alteradas com periodicidade não inferior a 90 dias e a obrigatoriedade de autenticações multifator;
- Definição de controlos de acesso baseados em roles, assumindo sempre o princípio de menor privilégio, garantindo que cada utilizador apenas tem acesso à informação estritamente necessária para as suas atividades. Destaca-se neste ponto a garantia de que cada aceleradora apenas tem acesso à informação dos beneficiários que apoia;
- Definição e implementação de uma política de retenção de dados, delimitando o período de tempo que a informação é armazenada, durante e após conclusão do projeto, onde e sob que condições (encriptação, anonimização, entre outros);
- Garantir a assinatura de acordos de confidencialidade por parte de todos os membros do projeto, salvaguardando legalmente o projeto Acelerar o Norte;
- Garantir, através de apoio às Aceleradoras e associações empresariais em que se inserem, que as redes e equipamentos nas quais operam cumprem os requisitos de antivírus, antimalware e sistemas de deteção de intrusos;
- Garantir que são implementadas estratégias de encriptação de dados e anonimização. Destaca-se neste ponto a anonimização ou mascaramento de dados quando seja necessário extrair informação de

todos os beneficiários, para análises, estudos de impacto ou monitorização do progresso do projeto;

- Definir os canais através dos quais é possível efetuar comunicações em nome do projeto, assim como localizações de armazenamento de informação e documentos de trabalho, de forma que estejam protegidos pelos procedimentos estabelecidos pelo projeto;
- Definir e implementar uma estratégia de backup de informação em funcionamento através dos canais estabelecidos no ponto anterior;
- Assegurar a existência de mecanismos de monitorização e registo de atividades, especialmente de comunicações e *download* de ficheiros;
- Refletir sobra a estratégia de continuidade de negócio, garantindo que estão reunidas as condições de retoma célere de atividade do projeto em caso de incidentes;
- Assegurar que todos os fornecedores ou entidades externas que possam ser subcontratados e por isso passarem a fazer parte do projeto Acelerar o Norte estão ao abrigo de acordos de confidencialidade e estão a par das boas práticas de gestão de informação confidencial.

**Membros do projeto e membros das Aceleradoras**

Por via de regra, o disposto neste sumário aplica-se, não só aos membros das Aceleradoras, como a todos os indivíduos das equipas que compõem o projeto Acelerar o Norte.

No entanto, dado o risco acrescido derivado da dispersão geográfica das equipas das Aceleradoras, acrescido de serem o elo de ligação principal com os *stakeholders* envolvidos no projeto, particularmente os beneficiários, são distinguidas situações relacionadas com a sua atividade.

As Aceleradoras terão acesso a um leque variado de informações sensíveis de vários atores nas regiões onde o projeto está presente, o que carecerá de uma gestão monitorizada e imparcial dos dados, evitando quebras de confidencialidade e partilha com terceiros, assim como potenciais favorecimentos. Os membros do projeto devem ser totalmente isentos na sua atuação e devem manter uma postura preventiva, de modo a cumprir com o disposto no Código de Ética e Conduta e no Manual de Boas Práticas de Gestão de Informação Confidencial.

Assim, são identificadas as seguintes recomendações:

- Não deve ser partilhada informação relativa ao projeto Acelerar o Norte com a Associação Empresarial que acolhe a Aceleradora, exceto nos casos em que esta informação seja de domínio público;
- Da mesma forma, não deve ser transferida informação que conste de bases de dados das Associações Empresariais para o projeto Acelerar o Norte, nem devem ser contactados, em nome do projeto, beneficiários identificados através das associações empresariais, enquanto os

mesmos não manifestarem o seu explícito interesse de fazer parte do projeto;

- As informações sobre o desenvolvimento do projeto, em qualquer etapa do mesmo, não podem ser partilhadas com as associações empresariais nem devem ser tornadas públicas através destas, sendo expressamente necessário alinhamento com a equipa de comunicação do projeto Acelerar o Norte em qualquer situação em que se pretenda fazer alusão ao projeto;
- Devem ser respeitados os procedimentos no que se refere aos canais de comunicação, plataformas de trabalho e armazenamento de informação, nomeadamente privilegiando a utilização da plataforma de projeto;
- Deve-se manter uma política de mesa limpa, certificando-se que, na ausência do local de trabalho principal por algum período de tempo, os dispositivos estão fechados e nenhuma informação está disponível ou acessível;
- Considerar a localização das equipas das Aceleradoras em espaços físicos (salas) distintos dos restantes colegas da Associação Empresarial, havendo uma separação formal e mitigando a possibilidade de quebra de confidencialidade não intencional;
- Trabalhar exclusivamente nos equipamentos facultados pelo projeto, evitando o acesso a plataformas de projeto através de dispositivos pessoais, como *smartphones* e computadores pessoais;
- Ainda, os equipamentos facultados pelo projeto servem o propósito de apoiar as atividades a realizar no âmbito do projeto, não podendo ser utilizados para outros fins ou cedidos a terceiros, mesmo que temporariamente;
- Os equipamentos devem ser protegidos, evitando ser colocados em locais não vigiados, ou ao alcance de terceiros, como sejam veículos, meios de transporte, estabelecimentos públicos, por qualquer período de tempo;
- Qualquer suspeita ou verificação de comportamentos que violem o disposto neste manual, ou outros procedimentos que venham a ser definidos pelo projeto, devem ser comunicadas de imediato à entidade empregadora.

## MAPEAMENTO DE PRINCIPAIS RISCOS RELACIONADOS COM A GESTÃO DE INFORMAÇÃO CONFIDENCIAL DO PROJETO ACELERAR O NORTE

Tendo por base as características do projeto, foram enumerados um conjunto de riscos relacionados com a gestão de informação confidencial no âmbito do mesmo.

Em primeiro lugar, importa definir o nível de risco como a combinação da probabilidade de ocorrência do evento e a gravidade do mesmo, levando, esta combinação, a uma escala de graduação de risco, conforme indicada na tabela abaixo.

Ainda, para cada potencial situação foram elencadas sugestões de medidas de mitigação e prevenção, tendo depois sido identificadas as medidas que se encontram implementadas no âmbito do projeto Acelerar o Norte, com o intuito de prevenir a ocorrência ou reduzir o impacto de cada risco.

**Escala de graduação de risco**

| GRAU DE RISCO | | | Probabilidade de ocorrência | | |
|---|---|---|---|---|---|
| | | | Baixa | Moderada | Alta |
| | | | 1 | 2 | 3 |
| Gravidade / Impacto | Baixa | 1 | 1 | 2 | 3 |
| | Moderada | 2 | 2 | 4 | 6 |
| | Alta | 3 | 3 | 6 | 9 |

| Riscos | Probabilidade de Ocorrência | Gravidade / Impacto | Nível de Risco | Sugestão de Medidas de Controlo / Prevenção | Medidas de Controlo / Mitigação implementadas |
|---|---|---|---|---|---|
| **Perda de informação confidencial e/ou comprometimento da continuação do projeto pela perda irreversível de informação devido a fenómenos naturais** | 1 | 3 | 3 | • Backup regular de dados, garantindo a existência de cópias online seguras<br>• Sensibilização para a preferência de trabalho em plataformas online colaborativas (plataforma de projeto, *onedrive*, *teams*, *sharepoint*, etc.) que permitam a recuperação de dados célere<br>• Medidas físicas de prevenção no local de trabalho, direcionadas ao hardware, de forma que não sejam comprometidas as infraestruturas (ex: curto-circuitos) | • Desenvolvimento e utilização de Plataforma CRM Acelerar o Norte, permitindo o trabalho em software colaborativo e online.<br>• Backup de dados da Plataforma CRM Acelerar o Norte efetuados ao nível do servidor, garantindo backups diários, semanais e das últimas 3 semanas |
| **Quebras de segurança ou divulgação de dados através de manipulação / engenharia social (*ex: phishing, whaling, baiting, scareware*, entre outras)** | 3 | 3 | 9 | • Backup regular de dados, garantindo a existência de cópias online seguras<br>• Capacitação dos membros do projeto para a identificação e reporte imediato de situações suspeitas<br>• Educação contínua da equipa sobre boas práticas de segurança cibernética, incluindo a identificação de *phishing* e outras técnicas de engenharia social. | • Backup de dados da Plataforma CRM Acelerar o Norte efetuados ao nível do servidor, garantindo backups diários, semanais e das últimas 3 semanas<br>• Capacitação das equipas sobre Boas Práticas de Gestão de Informação Confidencial e partilha de Manual de Boas Práticas de Gestão de Informação Confidencial |

| | | | | | |
|---|---|---|---|---|---|
| **Divulgação, corrupção, eliminação ou roubo de informação confidencial através da exposição de palavras-passe** | 2 | 3 | 6 | • Políticas de controlo de acessos, bem definidas e baseadas no critério do menor privilégio, de forma a tentar minimizar a abrangência de potenciais danos<br>• Registos de monitorização de atividade, passíveis de identificar e rastrear a atividades dos utilizadores<br>• Reforço da necessidade de estabelecer palavras-passe seguras e de evitar a escrita das mesmas em suporte físico que possa estar ao alcance de terceiros | • A utilização da plataforma CRM Acelerar o Norte contempla a separação de roles, entre aceleradoras de comércio digital, com cada uma das aceleradoras apenas visualizando as empresas que correspondem à sua área de atuação territorial e também entre membros da mesma aceleradora, com cada utilizador tendo acesso apenas às funcionalidades que são estritamente necessárias para o desempenho das suas funções.<br>• A plataforma CRM Acelerar o Norte, assim como as credenciais de projeto a utilizar em qualquer situação obrigam à definição de uma palavra-passe única com critérios de segurança (mín 8 caracteres, obrigatoriamente composta por letras, maiúsculas, números e caracteres especiais<br>• Política de atualização periódica das palavra-passe, com a obrigatoriedade de redefinição da mesma atingida a validade definida<br>• A plataforma CRM mantém um log de operações efetuadas pelos utilizadores, permitindo monitorizar a atividades dos mesmos, se necessário. |
| **Divulgação, corrupção, eliminação ou roubo de informação confidencial através de acessos de rede não autorizados** | 2 | 3 | 6 | • Estratégias de encriptação de dados inativos e em trânsito<br>• Implementação de palavras-passe seguras, autenticação multi-fator e controlo de acessos baseado em política de menor privilégio<br>• Evitar a ligação a redes sobre as quais não se conheçam as políticas de proteção de rede, como *firewalls* e SDI/SPI, como redes públicas<br>• Manter os softwares atualizados (instalação imediata de *patches)* Implementar políticas de identificação de vulnerabilidades de rede | • A utilização da plataforma CRM Acelerar o Norte contempla a separação de roles, entre aceleradoras de comércio digital, com cada uma das aceleradoras apenas visualizando as empresas que correspondem à sua área de atuação territorial e também entre membros da mesma aceleradora, com cada utilizador tendo acesso apenas às funcionalidades que são estritamente necessárias para o desempenho das suas funções.<br>• A plataforma CRM Acelerar o Norte, assim como as credenciais de projeto a utilizar em qualquer situação obrigam à definição de uma palavra-passe única com critérios de segurança (min. 8 caracteres, obrigatoriamente composta por letras, maiúsculas, números e caracteres especiais<br>• Política de atualização periódica das palavra-passe, com a obrigatoriedade de redefinição da mesma atingida a validade definida<br>• Encriptação dos dados em trânsito através do certificado digital SSL<br>• Obrigatoriedade de utilização de VPN (OpenVPN) do projeto, estabelecendo conexões mais seguras, que dificultam o acesso a informações confidenciais por parte de terceiros<br>• Proteção do software e de rede, assim como monitorização da infraestrutura tecnológica, assegurados ao nível do alojamento/servidor |

| | | | | | |
|---|---|---|---|---|---|
| **Apropriação de informação confidencial por parte de terceiros decorrente de conduta imprudente fora do âmbito digital** | 2 | 2 | 4 | • Sensibilização dos membros do projeto para os comportamentos preventivos no que se refere a exposição de informação, bloqueio de ecrãs, trabalho em espaços públicos, armazenamento e proteção de cópias físicas de informação confidencial<br>• Minimizar a necessidade da reprodução física de cópias ou de registo de informação em papel<br>• Sensibilização para a segurança dos equipamentos, nomeadamente não sendo deixados em momento algum em locais não vigiados, como automóveis, restaurantes, espaços públicos ou outros onde possam ser acedidos por terceiros | • Capacitação das equipas sobre Boas Práticas de Gestão de Informação Confidencial e partilha de Manual de Boas Práticas de Gestão de Informação Confidencial |
| **Perda de informação decorrente da destruição física dos equipamentos** | 1 | 2 | 2 | • Backup regular de dados, garantindo a existência de cópias online seguras<br>• Sensibilização para a segurança dos equipamentos, nomeadamente não sendo deixados em momento algum em locais não vigiados, como automóveis, restaurantes, espaços públicos ou outros onde possam ser acedidos por terceiros e danificados.<br>• Manutenção constante de inventário de equipamentos e registo de levantamento por parte de utilizadores, no sentido de identificar e desativar imediatamente o equipamento | • Capacitação das equipas sobre Boas Práticas de Gestão de Informação Confidencial e partilha de Manual de Boas Práticas de Gestão de Informação Confidencial<br>• Backup de dados da Plataforma CRM Acelerar o Norte efetuados ao nível do servidor, garantindo backups diários, semanais e das últimas 3 semanas |
| **Divulgação, corrupção, eliminação ou roubo de informação confidencial decorrente do roubo de equipamentos ou registos físicos** | 1 | 3 | 3 | • Backup regular de dados, garantindo a existência de cópias online seguras<br>• Implementação de estratégias de encriptação de dados, assim como de anonimização e mascaramento dos mesmos<br>• Sensibilização para a segurança dos equipamentos, nomeadamente não sendo deixados em momento algum em locais não vigiados, como automóveis, restaurantes, espaços públicos ou outros onde possam ser acedidos por terceiros e consequentemente furtados<br>• Manutenção constante de inventário de equipamentos e registo de levantamento por parte de utilizadores, no sentido de identificar e desativar imediatamente o equipamento | • Backup de dados da Plataforma CRM Acelerar o Norte efetuados ao nível do servidor, garantindo backups diários, semanais e das últimas 3 semanas<br>• Capacitação das equipas sobre Boas Práticas de Gestão de Informação Confidencial e partilha de Manual de Boas Práticas de Gestão de Informação Confidencial<br>• Encriptação dos dados em trânsito através do certificado digital SSL |

| | | | | | |
|---|---|---|---|---|---|
| **Quebra de confidencialidade, divulgação de dados e/ou danos à reputação do projeto decorrentes de partilhas públicas não autorizadas** | 1 | 3 | 3 | • Sensibilização dos colaboradores para os comportamentos no que se refere a contas de redes sociais, publicações, declarações aos media, entre outros, carecendo de aprovação da equipa de comunicação<br>• Sensibilização dos colaboradores no sentido de evitar a partilha de informação sobre as suas atividades de maneira informal em espaços públicos, ou com terceiros que não façam parte do projeto Acelerar o Norte<br>• Desenvolvimento de protocolos de resposta a incidentes mediáticos, para lidar rapidamente com casos que possam danificar a reputação do projeto ou dos seus parceiros e beneficiários | • Capacitação das equipas sobre Boas Práticas de Gestão de Informação Confidencial e partilha de Manual de Boas Práticas de Gestão de Informação Confidencial |
| **Disponibilização de dados confidenciais, de forma intencional, com o objetivo de beneficiar ou favorecer terceiros** | 2 | 3 | 6 | • Reforço do comportamento esperado pelos membros do projeto, constante do Código de Ética e Conduta, assim como das cláusulas de confidencialidade em vigor<br>• Políticas de controlo de acessos, bem definidas e baseadas no critério do menor privilégio, de forma a tentar minimizar o impacto de potenciais danos<br>• Desenvolvimento de políticas claras e procedimentos para identificar, prevenir e relatar suspeitas de intenções maliciosas de disponibilização de dados confidenciais.<br>• Implementação de medidas técnicas, como encriptação de dados, anonimização e mascaramento de dados<br>• Monitorização e rastreabilidade de acessos e atividades realizadas<br>• Estabelecimento de protocolos de resposta a incidentes para lidar rapidamente com casos de divulgação intencional, minimizando danos e reforçando a segurança. | • Capacitação das equipas sobre Boas Práticas de Gestão de Informação Confidencial e partilha de Manual de Boas Práticas de Gestão de Informação Confidencial<br>• A utilização da plataforma CRM Acelerar o Norte contempla a separação de roles, entre aceleradoras de comércio digital, com cada uma das aceleradoras apenas visualizando as empresas que correspondem à sua área de atuação territorial e também entre membros da mesma aceleradora, com cada utilizador tendo acesso apenas às funcionalidades que são estritamente necessárias para o desempenho das suas funções.<br>• A plataforma CRM mantém um log de operações efetuadas pelos utilizadores, permitindo monitorizar a atividades dos mesmos, se necessário. |
| **Divulgação, corrupção, eliminação ou roubo de informação confidencial decorrente de comportamento intencional e malicioso** | 2 | 3 | 6 | • Reforço do comportamento esperado pelos membros do projeto, constante do Código de Ética e Conduta, assim como das cláusulas de confidencialidade em vigor.<br>• Políticas de controlo de acessos, bem definidas e baseadas no critério do menor privilégio, de forma a tentar minimizar a abrangência de potenciais danos<br>• Desenvolvimento de políticas claras e canais para identificar, prevenir e relatar suspeitas de intenções maliciosas de disponibilização de dados confidenciais.<br>• Implementação de medidas técnicas, como encriptação de dados, anonimização e mascaramento de dados, para proteger a informação de acessos não autorizados. | • Capacitação das equipas sobre Boas Práticas de Gestão de Informação Confidencial e partilha de Manual de Boas Práticas de Gestão de Informação Confidencial<br>• A utilização da plataforma CRM Acelerar o Norte contempla a separação de roles, entre aceleradoras de comércio digital, com cada uma das aceleradoras apenas visualizando as empresas que correspondem à sua área de atuação territorial e também entre membros da mesma aceleradora, com cada utilizador tendo acesso apenas às funcionalidades que são estritamente necessárias para o desempenho das suas funções.<br>• Encriptação dos dados em trânsito através do certificado digital SSL |

| | | | | | |
|---|---|---|---|---|---|
| **Divulgação, corrupção, eliminação ou roubo de informação confidencial decorrente de comportamento acidental ou desconhecimento** | 3 | 3 | 9 | • Formação e capacitação dos membros do projeto no que se refere aos procedimentos de gestão de informação confidencial e disponibilização de conteúdos para consulta<br>• Reforço da utilização de canais de comunicação seguros<br>• Políticas de controlo de acessos, bem definidas e baseadas no critério do menor privilégio, de forma a tentar minimizar a abrangência de potenciais danos<br>• Monitorização de atividades e capacidade de rastreabilidade de operações efetuadas | • Capacitação das equipas sobre Boas Práticas de Gestão de Informação Confidencial e partilha de Manual de Boas Práticas de Gestão de Informação Confidencial<br>• A utilização da plataforma CRM Acelerar o Norte contempla a separação de roles, entre aceleradoras de comércio digital, com cada uma das aceleradoras apenas visualizando as empresas que correspondem à sua área de atuação territorial e também entre membros da mesma aceleradora, com cada utilizador tendo acesso apenas às funcionalidades que são estritamente necessárias para o desempenho das suas funções.<br>• A plataforma CRM mantém um log de operações efetuadas pelos utilizadores, permitindo monitorizar a atividades dos mesmos, se necessário. |
| **Divulgação, corrupção, eliminação ou roubo de informação confidencial decorrente de roubo de identidade ou comprometimento da identidade do utilizador no projeto** | 1 | 3 | 3 | • Estabelecimento de políticas rigorosas de gestão de palavras-passe, incentivando a utilização de senhas fortes e a atualização regular para evitar vulnerabilidades.<br>• Políticas de controlo de acessos, bem definidas e baseadas no critério do menor privilégio, de forma a tentar minimizar a abrangência de potenciais danos<br>• Implementação de estratégias de proteção de softwares e redes, como antivírus, antimalware, sistemas de deteção de intrusos<br>• Realização de auditorias regulares e testes de penetração para avaliar a eficácia dos protocolos de segurança e identificar áreas de melhoria na prevenção do roubo de identidade. | • Realização de auditorias regulares e testes de penetração para avaliar a eficácia dos protocolos de segurança e identificar áreas de melhoria na prevenção do roubo de identidade.<br>• A utilização da plataforma CRM Acelerar o Norte contempla a separação de roles, entre aceleradoras de comércio digital, com cada uma das aceleradoras apenas visualizando as empresas que correspondem à sua área de atuação territorial e também entre membros da mesma aceleradora, com cada utilizador tendo acesso apenas às funcionalidades que são estritamente necessárias para o desempenho das suas funções.<br>• A plataforma CRM Acelerar o Norte, assim como as credenciais de projeto a utilizar em qualquer situação obrigam à definição de uma palavra-passe única com critérios de segurança (min. 8 caracteres, obrigatoriamente composta por letras, maiúsculas, números e caracteres especiais<br>• Política de atualização periódica das palavra-passe, com a obrigatoriedade de redefinição da mesma atingida a validade definida<br>• Encriptação dos dados em trânsito através do certificado digital SSL<br>• Obrigatoriedade de utilização de VPN (OpenVPN) do projeto, estabelecendo conexões mais seguras, que dificultam o acesso a informações confidenciais por parte de terceiros<br>• Proteção do software e de rede, assim como monitorização da infraestrutura tecnológica, assegurados ao nível do alojamento/servidor |

| | | | | | |
|---|---|---|---|---|---|
| **Divulgação, corrupção, eliminação ou roubo de informação confidencial decorrente da utilização de dispositivos pessoais** | 2 | 3 | 6 | • Realização de auditorias regulares e testes de penetração para avaliar a eficácia dos protocolos de segurança e identificar áreas de melhoria na prevenção do roubo de identidade.<br>• Reforço da política de não utilização e dispositivos pessoais, já que os mesmos podem armazenar dados de acesso de forma automática, estando suscetíveis a roubos ou extravios e consequentemente a um potencial acesso à informação confidencial<br>• Estabelecimento de políticas rigorosas de gestão de palavras-passe, incentivando a utilização de senhas fortes e a atualização regular para evitar vulnerabilidades.<br>• Políticas de controlo de acessos, bem definidas e baseadas no critério do menor privilégio, de forma a tentar minimizar a abrangência de potenciais danos | • Capacitação das equipas sobre Boas Práticas de Gestão de Informação Confidencial e partilha de Manual de Boas Práticas de Gestão de Informação Confidencial<br>• A utilização da plataforma CRM Acelerar o Norte contempla a separação de roles, entre aceleradoras de comércio digital, com cada uma das aceleradoras apenas visualizando as empresas que correspondem à sua área de atuação territorial e também entre membros da mesma aceleradora, com cada utilizador tendo acesso apenas às funcionalidades que são estritamente necessárias para o desempenho das suas funções.<br>• A plataforma CRM Acelerar o Norte, assim como as credenciais de projeto a utilizar em qualquer situação obrigam à definição de uma palavra-passe única com critérios de segurança (mín 8 caracteres, obrigatoriamente composta por letras, maiúsculas, números e caracteres especiais<br>• Política de atualização periódica das palavra-passe, com a obrigatoriedade de redefinição da mesma atingida a validade definida |
| **Incumprimento de enquadramento legal (RGPD)** | 1 | 3 | 3 | • Desenvolvimento e manutenção de um registo de atividades de tratamento de dados, assegurando transparência e documentação adequada.<br>• Educação contínua da equipa sobre os princípios do RGPD e as suas responsabilidades na gestão de dados pessoais.<br>Estabelecimento de contratos e acordos claros com processadores de dados externos, garantindo que cumprem as obrigações do RGPD.<br>Designação de um encarregado de proteção de dados (DPO) para supervisionar a conformidade com o RGPD. | • Capacitação das equipas sobre Boas Práticas de Gestão de Informação Confidencial e partilha de Manual de Boas Práticas de Gestão de Informação Confidencial |
| **Falsificação ou contrafação de documentos que representem o projeto "Acelerar o Norte"** | 1 | 2 | 2 | • Implementação de medidas de segurança avançadas, como assinaturas digitais e códigos de autenticação ou palavras-passe de acesso, para proteger documentos.<br>• Estabelecimento de processos de verificação rigorosos para garantir a autenticidade de documentos emitidos em nome do projeto.<br>• Implementação de sistemas de gestão eletrónica de documentos para rastrear versões e alterações, garantindo a autenticidade ao longo do tempo. | • A plataforma CRM mantém um log de operações efetuadas pelos utilizadores, permitindo monitorizar a atividades dos mesmos, se necessário. |
| **Extravio ou furto de informação decorrente da realização não** | 2 | 2 | 4 | • Backup regular de dados, garantindo a existência de cópias online seguras<br>• Implementação de estratégias de encriptação de dados, assim como de anonimização e mascaramento dos mesmos | • Capacitação das equipas sobre Boas Práticas de Gestão de Informação Confidencial e partilha de Manual de Boas Práticas de Gestão de Informação Confidencial<br>Backup de dados da Plataforma CRM Acelerar o Norte efetuados ao |

| | | | | | |
|---|---|---|---|---|---|
| **controlada de cópias físicas ou digitais** | | | | • Sensibilização para a minimização da reprodução de cópias digitais ou físicas, dando primazia ao desenvolvimento das atividades no âmbito da plataforma do projeto<br>• Sensibilização para a segurança dos equipamentos, nomeadamente não sendo deixados em momento algum em locais não vigiados, como automóveis, restaurantes, espaços públicos ou outros onde possam ser acedidos por terceiros e consequentemente furtados<br>• Manutenção constante de inventário de equipamentos e registo de levantamento por parte de utilizadores, no sentido de identificar e desativar imediatamente o equipamento | nível do servidor, garantindo backups diários, semanais e das últimas 3 semanas |
| **Inexistência de políticas e procedimentos relativos à gestão do ciclo de vida dos utilizadores, incluindo a criação, atribuição, manutenção e atualização das contas de utilizadores do sistema** | 1 | 3 | 3 | • Desenvolvimento e implementação de políticas claras para a criação, atribuição, manutenção e atualização de contas de utilizadores do sistema.<br>• Manutenção constante de inventário de equipamentos e registo de levantamento por parte de utilizadores, no sentido de identificar e desativar imediatamente o equipamento aquando da cessação de vínculo laboral.<br>• Reforço de clausulas de confidencialidade cujo vigor se mantém após a cessação de atividade no projeto | • Política de atualização periódica das palavra-passe, com a obrigatoriedade de redefinição da mesma atingida a validade definida |
| **Comprometimento da capacidade de continuidade das atividades do projeto** | 1 | 3 | 3 | • Backup regular de dados, garantindo a existência de cópias online seguras e de cópias que se encontram em localizações externas com menor probabilidade de terem sido afetadas<br>• Realização de avaliações de risco regulares para identificar vulnerabilidades e implementar medidas preventivas que reduzam a probabilidade de comprometimento da atividade operacional.<br>• Estabelecimento de protocolos de resposta a incidentes para uma ação rápida e coordenada em caso de perturbações na atividade operacional. | • Backup de dados da Plataforma CRM Acelerar o Norte efetuados ao nível do servidor, garantindo backups diários, semanais e das últimas 3 semanas<br>• Proteção do software e de rede, assim como monitorização da infraestrutura tecnológica, assegurados ao nível do alojamento/servidor |

| | | | | | |
|---|---|---|---|---|---|
| **Formas de atuar diferentes ou incoerentes entre membros do projeto, decorrentes de uma comunicação de políticas e procedimentos ineficaz** | 3 | 3 | 9 | • Desenvolvimento de protocolos claros de comunicação, incluindo canais específicos para diferentes tipos de mensagens e níveis de urgência.<br>• Estabelecimento de reuniões regulares para alinhamento e partilha de atualizações, promovendo a coordenação entre as diferentes áreas do projeto.<br>• Adoção de ferramentas de gestão de projetos e colaboração para centralizar a informação e evitar dispersão.<br>• Designação de responsáveis pela comunicação interna e externa, assegurando que as mensagens sejam claras, consistentes e alinhadas com os objetivos do projeto. | • Capacitação das equipas sobre Boas Práticas de Gestão de Informação Confidencial e partilha de Manual de Boas Práticas de Gestão de Informação Confidencial |
| **Divulgação, corrupção, eliminação ou roubo de informação confidencial decorrente de uma política de eliminação de dados deficiente** | 2 | 2 | 4 | • Estabelecimento de procedimentos claros e seguros para a eliminação de dados confidenciais, seguindo as melhores práticas de destruição de informações sensíveis.<br>• Colaboração com empresas especializadas na eliminação segura de dados eletrónicos, garantindo a conformidade com padrões de segurança reconhecidos.<br>• Designação de responsáveis pela gestão da eliminação de dados, assegurando que o processo seja supervisionado e executado corretamente.<br>• Inclusão de cláusulas contratuais com fornecedores de serviços de eliminação de dados, garantindo a proteção das informações confidenciais. | • Parceria com entidade especializada no tratamento de dados pessoais |
| **Divulgação, corrupção, eliminação ou roubo de informação confidencial decorrente de uma rotina de manutenção de sistemas e softwares deficitária** | 2 | 3 | 6 | • Atualizações regulares de software para corrigir vulnerabilidades, melhorar a estabilidade e garantir a segurança dos sistemas. Monitorização constante da infraestrutura tecnológica para detetar precocemente sinais de falhas e permitir uma resposta rápida. | • Proteção do software e de rede, assim como monitorização da infraestrutura tecnológica, assegurados ao nível do alojamento/servidor |
| **Observância e passividade perante situações de atuação duvidosa ou perante o incumprimento das políticas definida** | 2 | 2 | 4 | • Reforço das políticas definidas para a gestão de informação confidencial e partilha de conteúdos para consulta frequente.<br>• Implementação de um procedimento de reporte eficiente e seguro de suspeitas de comportamentos irregulares<br>• Sensibilização contínua das equipas sobre a importância do reporte imediato de incidentes de segurança e os procedimentos a seguir. | • Capacitação das equipas sobre Boas Práticas de Gestão de Informação Confidencial e partilha de Manual de Boas Práticas de Gestão de Informação Confidencial |

aceleraronorte.pt

CONSÓRCIO

CCP CONFEDERAÇÃO DO COMÉRCIO E SERVIÇOS PORTUGAL

AEP ASSOCIAÇÃO EMPRESARIAL DE PORTUGAL Câmara de Comércio e Indústria

AHRESP Respostas para o futuro desde 1896

ACEPI ASSOCIAÇÃO ECONOMIA DIGITAL

FINANCIAMENTO

PRR Plano de Recuperação e Resiliência

REPÚBLICA PORTUGUESA

Financiado pela União Europeia NextGenerationEU