MANUAL DE CIBERSEGURANÇA

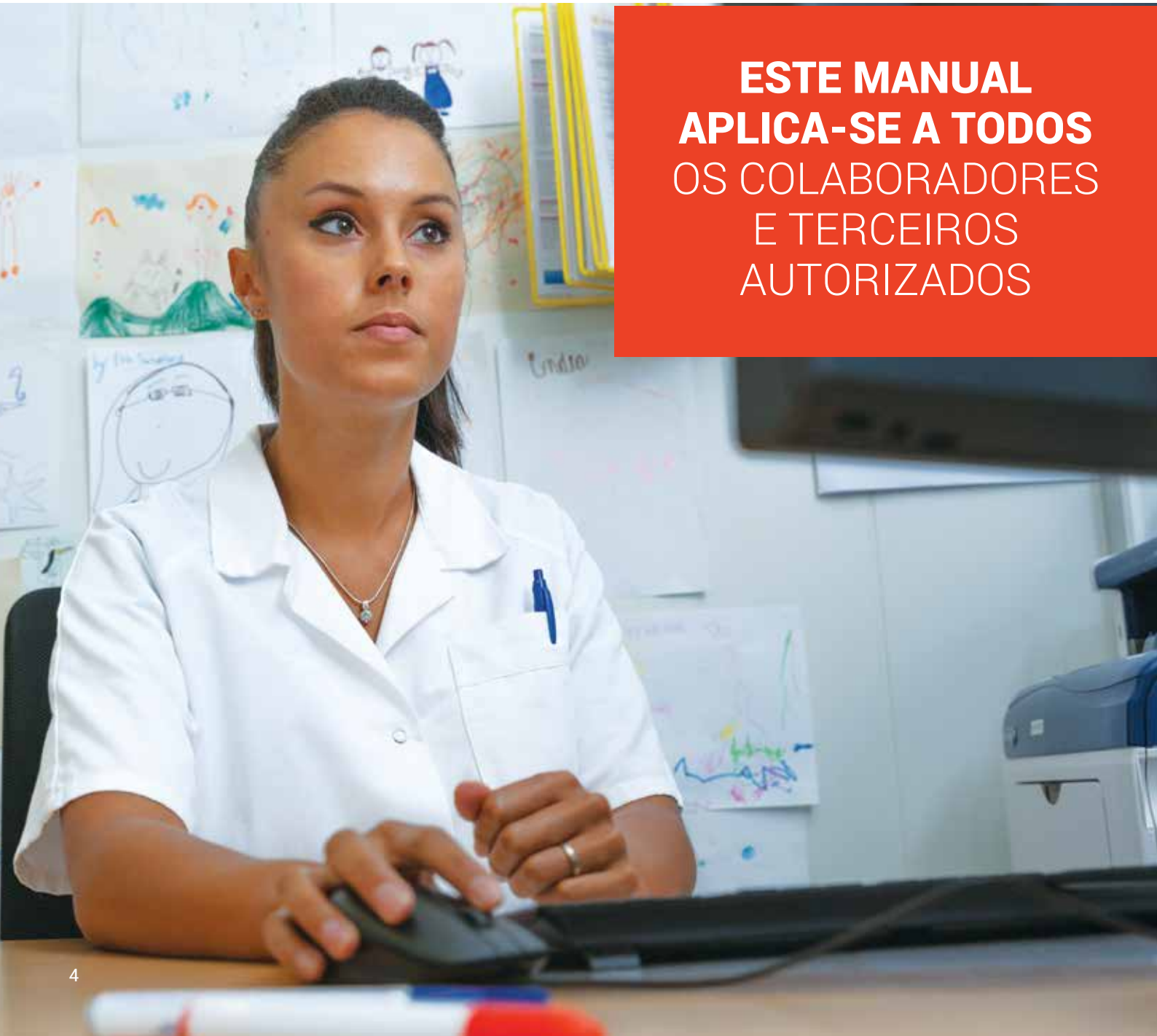
GRUPO UNILABS

Unilabs

ÍNDICE

1. INTRODUÇÃO

O Manual de Cibersegurança sustenta a Política de Cibersegurança da Unilabs e outros procedimentos, especificando as regras que garantam o uso adequado e seguro dos recursos digitais da Unilabs (qualquer dispositivo informático, aplicação, ferramenta ou serviço).



ESTE MANUAL APLICA-SE A TODOS OS COLABORADORES E TERCEIROS AUTORIZADOS

2. ALCANCE

A segurança cibernética é uma preocupação e responsabilidade de todos.
Este manual aplica-se a:

- Todas as empresas do Grupo Unilabs.
- Todos os colaboradores e terceiros autorizados, como colaboradores não empregados, consultores, colaboradores independentes, fornecedores ou clientes (denominados vulgarmente como "utilizadores") que utilizem recursos digitais da Unilabs.

3. CONFORMIDADE

O não cumprimento das disposições deste regulamento pode resultar em ações disciplinares, incluindo, mas não limitado a, rescisão com colaboradores da Unilabs e rescisão de relações com terceiros autorizados.

As regras apresentadas neste manual estão sujeitas à legislação e os regulamentos em vigor.

4. PRINCÍPIOS GERAIS

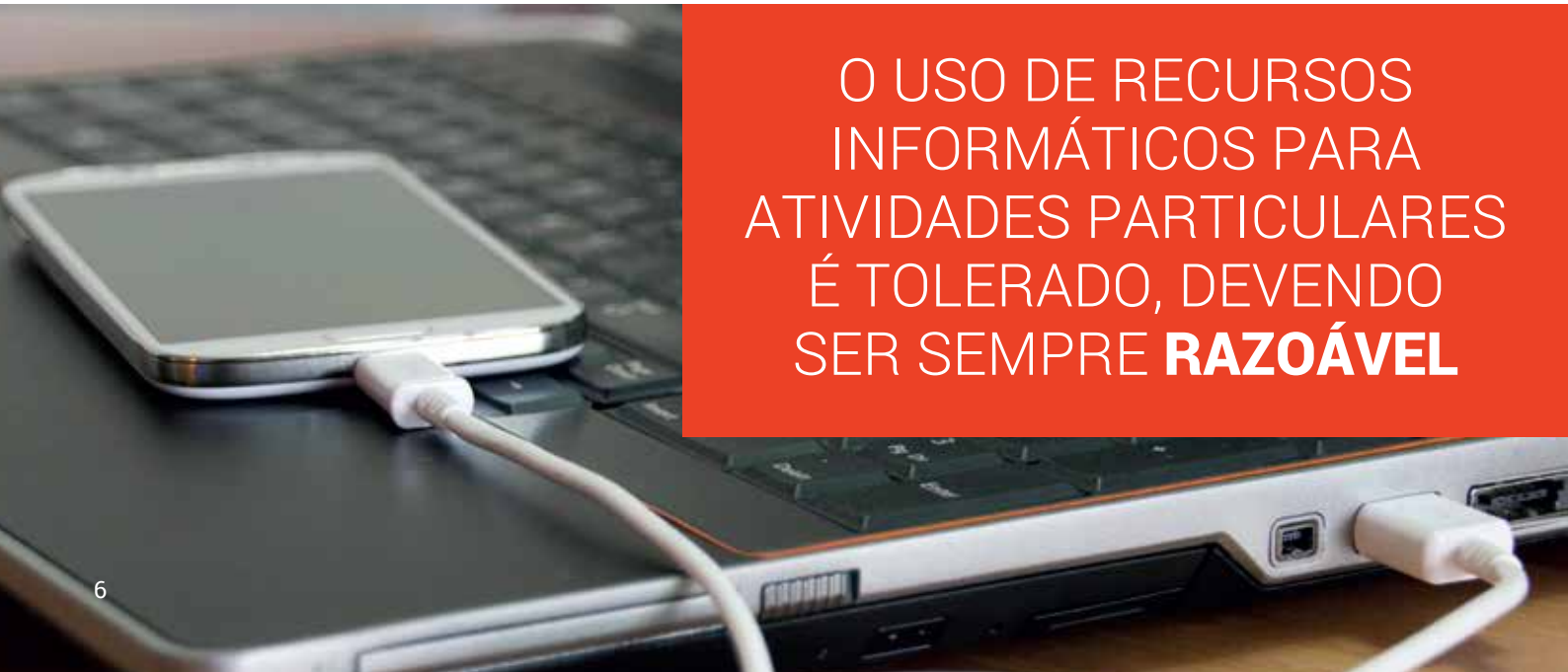
4.1

4.1.1 Utilização profissional.
Quando os utilizadores recebem acesso a recursos digitais, é apenas para o exercício das atividades profissionais.
Esses recursos pertencem à Unilabs e qualquer informação, ficheiro ou mensagem armazenados ou transmitidos através deles são considerados profissionais, pertencendo então à Unilabs.
A utilização de dispositivos de consumo no trabalho (por exemplo, smartphones ou tablets) está sujeita às regras de BYOD (Traga o seu dispositivo pessoal) apresentadas no capítulo 8.

4.1.2 A segurança cibernética é uma preocupação de todos.
Todos devem contribuir para a segurança da Unilabs. O nível de segurança global é como uma corrente, sendo tão forte quanto o seu elo mais fraco.

4.1.3 Responsabilidade individual.
Cada utilizador é responsável pela utilização segura, apropriada e legal de recursos feitos com o seu acesso individual, incluindo a utilização de comunicações eletrónicas e da Internet por meio de recursos digitais da empresa.

4.1.4 Utilização particular.
A utilização de recursos informáticos para atividades particulares (por exemplo, envio de e-mails, navegação na Web, armazenamento de informações particulares e similares) é tolerada, devendo permanecer razoável, ocasional, e não deverá violar leis e regulamentos, afetar operações de trabalho, a segurança de recursos digitais ou os interesses da Unilabs. Os utilizadores são responsáveis por usar do bom senso relativamente à razoabilidade do uso pessoal.



O USO DE RECURSOS INFORMÁTICOS PARA ATIVIDADES PARTICULARES É TOLERADO, DEVENDO SER SEMPRE **RAZOÁVEL**

4.2 CUMPRIMENTO DA LEGISLAÇÃO EM VIGOR

4.2.1 Cumprimento da legislação.
O utilizador deve cumprir toda a legislação em vigor relacionada com a utilização de ativos digitais, tais como (mas não limitado a):

- Leis e regulamentos de saúde;
- Dados pessoais (ver regra 4.2.2);
- Não utilização dos sistemas de informação para cometer crimes, incluindo fraude;
- Propriedade intelectual e direitos de autor;
- Leis do trabalho;
- Outras leis e regulamentos aplicáveis.

4.2.2 Regulamento Geral de Proteção de Dados (GDPR) e leis de proteção de dados pessoais.
A Unilabs compromete-se a recolher e processar dados sobre os seus colaboradores e outros utilizadores autorizados (p. ex. subcontratados, clientes, pacientes) de forma justa e legal, e apenas para fins legitimamente comerciais. Antes de criar qualquer ficheiro que contenha dados pessoais (p. ex. nome, data de nascimento, endereço de e-mail, etc.), os utilizadores devem garantir que estão em conformidade com a Política da Proteção de dados do Grupo Unilabs.

4.2.3 Informações sobre proteção de dados pessoais.
O departamento de informática da Unilabs processa os dados pessoais dos utilizadores para fins de gestão informática. Por favor, consulte o Apêndice 1 para obter mais informações sobre estas atividades de processamento.

4.2.4 Utilização Ética.
Os recursos digitais não devem ser utilizados de forma ilegal ou de forma a comprometer a reputação da Unilabs, seja para descarregar, aceder ou enviar material ilegal, atos de abuso e violência escritos ou verbais, atos contrários às regras éticas, incluindo, mas não se limitando a:

- Pornografia de qualquer tipo;
- Calúnia e abuso;
- Incitação a crimes e ofensas, discriminação, ódio ou violência;
- Assédio;
- Desculpabilização de crimes;
- Comprometer crianças ou expô-las a material violento ou pornográfico;
- Incitação à posse, consumo ou tráfico de substâncias proibidas.

Os recursos digitais devem sempre ser usados em conformidade com o Código de Conduta da Unilabs.

4.3 COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA

Qualquer incidente de segurança (i.e, violação de dados, atividade suspeita ou violação da Política de Cibersegurança da Unilabs e procedimentos relacionados, incluindo este regulamento), seja acidental ou intencional, deve ser comunicado imediatamente ao departamento de informática local.

Incidentes de segurança incluem (mas não estão limitados a):

- E-mail suspeito ou não solicitado (p. ex. phishing, spoofing);
- Malware;
- Roubo ou perda de um dispositivo com informações da Unilabs (computador, smartphone, BYOD, pen USB, etc.);
- Informação solicitada através de meios não convencionais;
- Fuga de dados, ou seja, informações divulgadas a público inadequado;
- Violação acidental ou inadvertida de regras de cibersegurança.

Os incidentes de segurança são geridos de acordo com o Procedimento de Gestão de Incidentes de Segurança do Unilabs. Uma violação de dados pessoais é um tipo de incidente de segurança e, além disso, deve seguir o Procedimento de Notificação de Violação de Dados de Grupo.

A CHEFIA DIRETA É RESPONSÁVEL PELA ATRIBUIÇÃO, ATUALIZAÇÃO E CANCELAMENTO OPORTUNO DOS DIREITOS DE ACESSO PARA OS SEUS SUBORDINADOS E OUTROS UTILIZADORES AUTORIZADOS, DOS QUAIS O É RESPONSÁVEL.

5. ACESSO A RECURSOS DIGITAIS

5.1 NOMES DE UTILIZADOR E PALAVRAS-PASSE

5.1.1 Nomes de utilizador pessoais
Cada utilizador recebe um nome de utilizador e palavra-passe pessoais para aceder à rede e a aplicações da Unilabs necessários para exercer as suas atividades. Os nomes de utilizadores e palavras-passe pessoais são estritamente individuais e são consideradas informações confidenciais, por isso, não devem ser partilhados entre utilizadores e as palavras-passe não devem ser transmitidas a ninguém, incluindo elementos do departamento de informática.

5.1.2 Responsabilidade individual
Cada utilizador é responsável pelas ações realizadas com o seu nome de utilizador e palavra-passe.

5.1.3 Ciclo de vida do utilizador.
A Chefia direta é responsável pela atribuição, atualização e cancelamento oportuno dos direitos de acesso para os seus subordinados e outros utilizadores autorizados, dos quais a Chefia é responsável. Isto é efetuado enviando os formulários de solicitação apropriados para o departamento de informática e por meio de uma revisão regular (pelo menos anual) dos acessos dos seus subordinados. Os direitos de acesso chegam ao fim a partir do momento em que a atividade profissional que justificou esse acesso é suspensa ou termina (por exemplo, rescisão do contrato, final da atribuição, alteração funcional ou de departamento).

Quando tais atividades são executadas pelo departamento de Recursos Humanos, devem levar em consideração todo o ciclo de vida dos direitos de acesso (criação e exclusão de utilizadores, alteração de acesso quando o utilizador muda de posição, etc.).

OS NOMES DE UTILIZADOR E PALAVRAS-PASSE **NÃO DEVEM SER PARTILHADOS** ENTRE UTILIZADORES, E AS PALAVRAS-PASSE NÃO DEVEM SER TRANSMITIDAS A NINGUÉM

5.1.4 Regras de palavras-passe
Os utilizadores devem:

- Escolher uma palavra-passe que seja difícil de descobrir: com pelo menos 8 caracteres, contendo pelo menos uma combinação de letras (maiúsculas e minúsculas), números e caracteres especiais;
- Alterar a sua palavra-passe pelo menos a cada 3 meses, ou imediatamente se houver suspeita de invasão;
- Não escrever as palavras-passe em papel;
- Não usar palavras-passe triviais, tais como nomes simples, palavras ou informações pessoais, que possam ser facilmente descobertas;
- Não usar "guardar palavra-passe" (p.ex. no navegador da Internet) para facilitar o processo de autenticação.

5.2 PERMISSÕES DE ACESSO

5.2.1 Nível de autorização.
Cada utilizador deve aceder apenas às informações para as quais tem autorização de acesso. Se um utilizador considerar que o seu nível de autorização é insuficiente, deverá solicitar ao gestor que modifique a autorização específica de acordo. Os utilizadores não devem tentar aceder por meio de informações sigilosas ou impróprias às quais não tenham acesso autorizado.

5.2.2 Suspensão.
As permissões de acesso podem ser suspensos por um dos seguintes motivos:

- Palavras-passe erradas são inseridas consecutivamente;
- O utilizador ficou inativo por um longo período;
- As permissões de acesso expiraram;
- Por solicitação formal dos Recursos Humanos, do proprietário da aplicação ou do Responsável pela Segurança da Informação.

Nestes casos, o utilizador deve entrar em contacto com o suporte informático local e aguardar instruções para reativar as suas permissões.

5.2.3 Procedimento de Gestão de Acesso do Utilizador
Quaisquer permissões de acesso devem ser geridas em conformidade com o Procedimento de Gestão de Acesso do Utilizador da Unilabs. Este procedimento define regras para a identificação, autenticação e autorização de utilizadores, de forma garantir que apenas pessoas autorizadas tenham acesso a aplicações comerciais, sistemas de informação, redes e dispositivos informáticos.

6. UTILIZAÇÃO DE RECURSOS DIGITAIS

6.1 HARDWARE E SOFTWARE

6.1.1 Hardware da empresa

Qualquer pessoa que receba um equipamento informático da Unilabs (posto de trabalho, computador portátil, dispositivo móvel, tablets, disco rígido externo, etc.) deve:

- Usar apenas ferramentas fornecidas ou autorizadas pelo departamento de informática para ligar o computador à rede Unilabs;
- Bloquear a sessão (e fechar aplicações) assim que saia do computador, mesmo que seja por um breves instantes. Os utilizadores não devem confiar no encerramento de sessão automático;
- Reiniciar o equipamento sem atrasos desnecessários quando solicitado, a fim de atualizar as configurações de segurança;
- Terminar sessão ou desligar o computador quando sair do escritório no final do dia;
- Não modificar a configuração de segurança do computador, especialmente no que diz respeito a configurações de antivírus e parâmetros de segurança;
- Não ligar (com ou sem fios) aos recursos da Unilabs qualquer equipamento (computador portátil, bem como switches, modems, smartphones, etc.), que não tenha sido fornecido ou aprovado pelo departamento de informática.

6.1.3 Software

Os utilizadores recebem ferramentas de software e aplicações necessárias para o desempenho das suas atividades. Os utilizadores devem:

- Respeitar as questões relacionadas com licenças e propriedade intelectual, não fazendo cópias de software licenciado à Unilabs para uso em computadores que não sejam da Unilabs;
- Não descarregar ou instalar software e aplicações adicionais por conta própria; para qualquer necessidade específica deve entrar em contato com o departamento de informática local;
- Não usar jogos, partilha de ficheiros peer-to-peer ou software de monitorização de rede nos postos de trabalho ou servidores da Unilabs, a menos que seja especificamente autorizado pelo responsável pelo departamento de informática local.

6.1.3 Aplicações de nuvem particulares

Os utilizadores não devem usar aplicações ou serviços particulares da Internet (por exemplo, o Dropbox) sem aprovação prévia do departamento de informática local.

6.1.4 Devolução de recursos digitais

Ao sair da Unilabs ou quando solicitado, o utilizador deve devolver todos os recursos digitais, incluindo hardware e outros dispositivos digitais, que lhe foram atribuídos. Esses recursos e todos os dados armazenados neles pertencem à empresa e é da responsabilidade do utilizador eliminar qualquer informação particular.

OS UTILIZADORES DEVEM
TERMINAR A SUA SESSÃO
ASSIM QUE DEIXAM
O COMPUTADOR

6.2 CÓPIAS DE SEGURANÇA E ARMAZENAMENTO

6.2.1 Não armazenar dados localmente
Sempre que possível, os utilizadores devem evitar armazenar dados localmente nos computadores e usar preferencialmente o serviço de armazenamento de ficheiros aprovado pela Unilabs (partilhas de rede ou ferramentas de colaboração).

6.2.2 Cópias de segurança
Os utilizadores são responsáveis pela utilização de partilhas de rede fornecidas pelo departamento de informática, a fim de armazenar e garantir uma cópia de segurança efetiva dos dados. Os dados armazenados localmente (ou seja, no disco rígido do computador) não são automaticamente guardados na cópia de segurança e podem ser perdidos caso sejam acidentalmente excluídos ou caso o computador tenha algum problema (malware, roubo ou perda do computador).

6.3 USO DE DISPOSITIVOS REMOVÍVEIS (DISCOS RÍGIDOS, PENS USB, DVD, CD)

6.3.1 Não ligar dispositivos externos
Os utilizadores não devem permitir que entidades externas liguem dispositivos externos, como dispositivos de armazenamento USB ou um disco rígido, ao seu computador. Nestas situações, os ficheiros devem ser redirecionados para o serviço de partilha de ficheiros aprovado pela Unilabs (e-mail ou ferramenta de colaboração) ou usar o seu próprio dispositivo de armazenamento USB para obter uma cópia do documento.

6.3.2 Dispositivos de armazenamento USB
Os dispositivos de armazenamento USB são uma ferramenta conveniente para trocar informações com terceiros, mas também são voláteis e não devem ser usadas como forma de cópia de segurança.

OS UTILIZADORES SÃO RESPONSÁVEIS POR UTILIZAR **PARTILHAS DE REDE** PARA ARMAZENAR E GARANTIR UMA **CÓPIA DE SEGURANÇA** BEM SUCEDIDA DOS SEUS DADOS

Como consequência:

- As informações devem ser guardadas apenas temporariamente;
- Antes de transmitir informações a terceiros, os utilizadores devem remover do dispositivo de armazenamento USB qualquer informação não destinada ao destinatário;
- Depois de transmitir informações a terceiros, os utilizadores devem eliminar o conteúdo do dispositivo de armazenamento USB;
- Os utilizadores devem evitar o armazenamento de dados pessoais;
- No caso de informações confidenciais ou sensíveis serem armazenadas num dispositivo de armazenamento USB, essas informações devem ser encriptadas.

6.3.3 Proteção de dispositivos removíveis

Os utilizadores devem proteger os seus dispositivos removíveis contra roubo, perda ou uso não autorizado, não os deixando sem supervisão ou, caso contrário, mantendo-os bloqueados.

6.3.4 Descarte

Todo o dispositivo removível inutilizado deve ser devolvido ao departamento que o forneceu. Não deve ser deitado em contentores de lixo públicos.

6.4 NO ESCRITÓRIO / FORA DO ESCRITÓRIO

6.4.1 Proteção de dispositivos móveis

Os utilizadores devem proteger os seus dispositivos móveis (computadores portáteis, smartphones e outros equipamentos informáticos) contra roubo, perda, acidentes e uso não autorizado:

- Os dispositivos não devem ser deixados sem supervisão, tanto no escritório como em locais públicos, a menos que estejam protegidos em armazenamento fechado ou com um cabo anti-roubo. Os cofres fornecidos nos quartos de hotel, se houverem, devem ser usados quando os deixa sem supervisão no quarto;
- Os dispositivos móveis não devem ser deixados em carros estacionados (mesmo quando trancados);
- Os dispositivos devem ser bloqueados quando não estiverem em uso, e o seu desbloqueio deve ser permitido apenas mediante a inserção da palavra-passe;
- Os filtros de privacidade são fornecidos pelo departamento de informática para impedir a leitura de quem passa pelas costas do utilizador. Devem ser usados em computadores portáteis, especialmente quando se trabalha em locais públicos.

6.4.2 Ligação à rede Unilabs

Durante viagens de negócios mais alargadas, os utilizadores devem ligar (pelo menos semanalmente) o seu computador à rede Unilabs, remotamente, se necessário, para garantir que as proteções de segurança sejam atualizadas no sistema.

7. PARTILHA DE INFORMAÇÕES

7.1 CONFIDENCIALIDADE

7.1.1 Dever de confidencialidade.
Todos os funcionários devem cumprir com o seu dever de confidencialidade e sigilo em relação às informações que chegam ao seu conhecimento.

7.1.2 Antes de divulgar informações
O funcionário deve:

- Verificar com o proprietário das informações o nível de confidencialidade da informação que está prestes a divulgar e aplicar as regras de divulgação de acordo com o Procedimento de Classificação e Tratamento de Informações da Unilabs;
- Ter em atenção a identidade da pessoa a quem está prestes a divulgar a informação;
- Garantir que a informação só chega ao destinatário pretendido, especialmente quando em locais públicos ou por telefone;
- Verificar o público e evitar partilhar todo o seu ambiente de trabalho com um público não confiável durante reuniões de vídeo ou audioconferência.

7.1.3 Engenharia social
Os cibercriminosos usam vários meios para reunir informações úteis: a partir da Internet, por telefone ou por e-mail, para poderem realizar ciberataques.
O funcionário deve:

- Não divulgar informações confidenciais relacionadas com a Unilabs na Internet por meio de redes sociais, fóruns on-line ou chats, por exemplo;
- Não divulgar informações, por mais insignificantes que pareçam, a alguém que não conheça, confie ou reconheça.

7.2 MANUSEAMENTO DE DOCUMENTOS SENSÍVEIS

7.2.1 Classificação do documento
Todos os documentos devem ser classificados por um nível de confidencialidade (público, interno, restrito, altamente confidencial), de acordo com o Procedimento de Classificação e Tratamento de Informações da Unilabs, que prevê regras para determinar o nível de classificação com base nos requisitos de restrição de acesso e impacto para a empresa em caso de divulgação. Quando o documento é criado, este nível deve ser indicado de forma clara no mesmo.

7.2.2 Manuseamento de documentos
Os documentos devem ser manuseados cuidadosamente de acordo com seu nível de confidencialidade e de acordo com o Procedimento de Classificação e Tratamento de Informações da Unilabs. Esta política determina como divulgar, enviar, armazenar e eliminar informações com base no nível de confidencialidade. Os documentos confidenciais ou sensíveis, em especial, devem ser encriptados e não partilhados ou publicados num espaço público sem se verificar quem tem acesso ao mesmo. Em caso de dúvida, o utilizador deve verificar o seu nível de sensibilidade junto da pessoa que distribuiu ou criou o documento.

7.2.3 Acesso a documentos

Os utilizadores não devem tentar aceder a informações confidenciais que não lhe sejam destinadas. Se informações confidenciais chegarem ao seu conhecimento inadvertidamente, deverão informar o proprietário da informação e não divulgá-la a ninguém, de acordo com sua obrigação de confidencialidade.

NUNCA CLIQUE EM LINKS OU ANEXOS DE E-MAILS SUSPEITOS

7.3 E-MAIL

7.3.1 Receção de e-mails

Ao receber e-mails, os utilizadores devem:

- Confirmar novamente a identidade do remetente se o conteúdo do e-mail for suspeito. Por exemplo, devem verificar a assinatura digital do remetente, caso exista, ou responder ao seu contacto habitual, previamente verificado (ou seja, um endereço de e-mail ou número de telefone validado).
- Nunca clicar em links ou anexos de e-mails suspeitos. Um e-mail suspeito talvez seja um que não esteja relacionado com o trabalho normal, que vem de um remetente desconhecido ou que contém instruções não convencionais.
- Não responder a e-mails não solicitados (spam).
- Reportar e-mails suspeitos e todos os e-mails com informações ilegais ou ofensivas.

7.3.2 Envio de e-mails

Antes de enviar ou encaminhar e-mails, os utilizadores devem:

- Verificar o nível de confidencialidade das informações no e-mail e nos ficheiros anexados;
- Encriptar e-mails que contenham informações confidenciais ou sensíveis;
- Limitar o envio de e-mails apenas para as pessoas que precisam de o receber (ou seja, utilizar o "responder a todos" com moderação);
- Verificar se os destinatários de e-mail estão corretos e se os endereços de e-mail estão escritos corretamente;
- Não enviar nem encaminhar spam, e-mails não solicitados ou em cadeia, exceto para relatar algum incidente ou anomalia;
- Não enviar e-mails profissionais de um endereço de e-mail que não seja da Unilabs;
- Não encaminhar automaticamente e-mails para uma caixa de correio externa, como um endereço de e-mail particular.

7.3.3 Uso profissional

Os utilizadores não devem usar ou comunicar os endereços de e-mail da Unilabs para atividades não profissionais, uma vez que aumenta o risco de receber e-mails não solicitados e mal-intencionados.

8. SMARTPHONES, TABLETS E BYOD
(BRING YOUR OWN DEVICE - TRAGA O SEU PRÓPRIO DISPOSITIVO)

Todos os dispositivos BYOD ou de consumo (por exemplo, tablets e smartphones, excluindo computadores portáteis), que são de propriedade de colaboradores e utilizados para fins comerciais, estão vinculados às regras deste Manual de Cibersegurança. Este capítulo visa esclarecer como as regras se aplicam especificamente a cada dispositivo.

8.1 VALIDAÇÃO PELO DEPARTAMENTO DE INFORMÁTICA

Por norma, não se pode ligar um dispositivo do colaborador à rede Unilabs (exceto à rede Wifi de convidado) ou armazenar quaisquer dados da Unilabs (incluindo e-mails das caixas de correio). Para se ligar à rede da Unilabs ou aceder a dados da Unilabs (incluindo e-mails das caixas de correio), o dispositivo do colaborador deve ser especificamente autorizado e registado no departamento de informática, antes de ser ligado à rede da Unilabs. O utilizador deve permitir que o departamento de informática proteja o dispositivo de acordo com os padrões de segurança da empresa.

8.2 GESTÃO DE DISPOSITIVOS MÓVEIS

Os utilizadores reconhecem que os dispositivos de consumo utilizados para fins profissionais contêm dados da empresa. Como consequência, a segurança dos dispositivos é monitorizada (possivelmente remotamente) pelo departamento de informática, a que se reserva o direito de:

- Verificar o dispositivo quanto a atividades não autorizadas ou informação ilícita. Se for necessário, a empresa pode confiscar e inspecionar o dispositivo;
- Gerir remotamente o dispositivo (por exemplo, por meio de soluções de gestão de dispositivos móveis) e implementar controlos técnicos;
- Acionar um sistema de segurança remoto ou limpeza, por exemplo, no caso do dispositivo ser perdido ou roubado, o que significa que todos os dados contidos no dispositivo poderão ser eliminados, sem a responsabilidade da Unilabs pela perda de dados pessoais.

8.3 RESPONSABILIDADES DO UTILIZADOR

Os utilizadores de dispositivos de consumo são obrigados a:

- Proteger os dados da empresa no dispositivo durante todo o ciclo de vida do mesmo;
- Comunicar imediatamente incidentes reais ou suspeitos relacionados com o dispositivo (p. ex., perda ou roubo, divulgação não autorizada de informações);
- Entrar em contato com o departamento de informática para qualquer problema de hardware ou software antes de levar o dispositivo ao fornecedor;
- Informar o departamento informático local sobre qualquer alteração de dispositivo para permitir a remoção remota de todas as informações da empresa do dispositivo antigo.

8.4 CONTROLOS DE SEGURANÇA

Os dispositivos de consumo utilizados para fins profissionais estão sujeitos a controlos de segurança específicos, como a exigência de uma palavra-passe e o bloqueio automático do dispositivo.

8.5 PROTEÇÃO DE DISPOSITIVOS

Os utilizadores de dispositivos de consumo devem:

- Instalar e manter atualizadas as proteções anti-malware e anti-vírus.
- Manter o dispositivo atualizado com a versão mais recente do sistema operativo e instalar as atualizações de segurança quando solicitado.
- Não adulterar as configurações de segurança nem utilizar software não aprovado nos dispositivos (normalmente chamado de "jailbreaking").
- Não deixar o dispositivo sem supervisão e bloqueá-lo sempre que não estiver em uso.
- Não partilhar o dispositivo e palavra-passe com outras pessoas (incluindo familiares e amigos).
- Não sincronizar o dispositivo com dispositivos desconhecidos, como dispositivos em ciber-cafés, etc.
- Não ativar o Bluetooth em locais públicos.

9. MONITORIZAÇÃO

9.1 DIREITO DE MONITORIZAR

A Unilabs tem o direito de monitorizar e controlar, de acordo com a legislação em vigor, o uso de quaisquer recursos e softwares relevantes, bem como as partilhas transmitidas pelas redes de comunicação, com o objetivo de garantir o funcionamento correto do sistema de informação, segurança e os interesses da empresa.

9.2 PROFISSIONAIS DE INFORMÁTICA

Estas operações são realizadas sob a responsabilidade de profissionais de informática, vinculados a uma obrigação de sigilo e confidencialidade.

9.3 CONTROLOS PROPORCIONAIS E NÃO DISCRIMINATÓRIOS

As atividades de monitorização são proporcionais ao seu objetivo e conduzidas de forma não discriminatória, a menos que haja uma razão comercial válida, p. ex. uma suspeita de fraude ou ação maliciosa. Essas operações podem incluir o acesso a ficheiros de registo, como registo do e-mail ou de acesso à Internet, que poderão conter dados pessoais. Caso sejam detetadas anomalias durante as verificações, o utilizador envolvido será avisado.

9.4 CIRCUNSTÂNCIAS ESPECIAIS

Em caso de uso ilícito sob circunstâncias graves ou de perigo para o correto funcionamento dos sistemas digitais, da sua segurança ou dos interesses do Grupo, a Unilabs pode precisar de aceder aos ficheiros ou mensagens dos utilizadores, sem a presença dos mesmos, e tomar as medidas apropriadas para isolar os ficheiros afetados, se houver (p. ex., infecção por vírus).

9.5 CONTINUIDADE

O acesso aos ficheiros ou caixas de correio de um utilizador pode ser concedido a sua Chefia direta para garantir a continuidade das atividades nas seguintes situações:

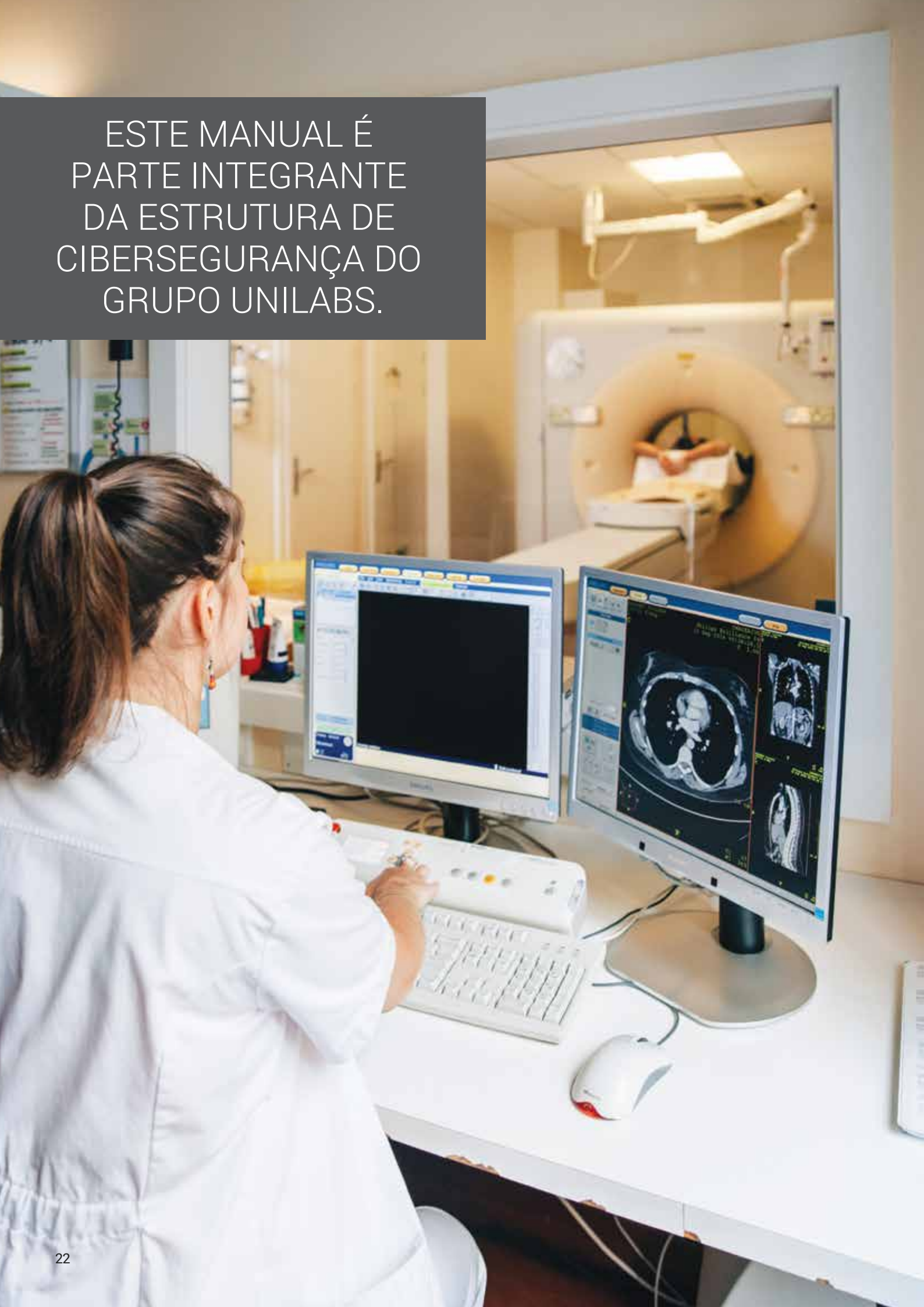
- O utilizador deixou a empresa permanentemente.
- O utilizador encontra-se num regime de licença inesperada ou alargada. Nestas circunstâncias, o utilizador envolvido será avisado assim que seja possível.

O período de retenção da pasta pessoal ou caixa de correio de um utilizador que deixou a empresa permanentemente é de 6 meses no máximo .

9.6 FICHEIROS DE REGISTO DOS UTILIZADORES

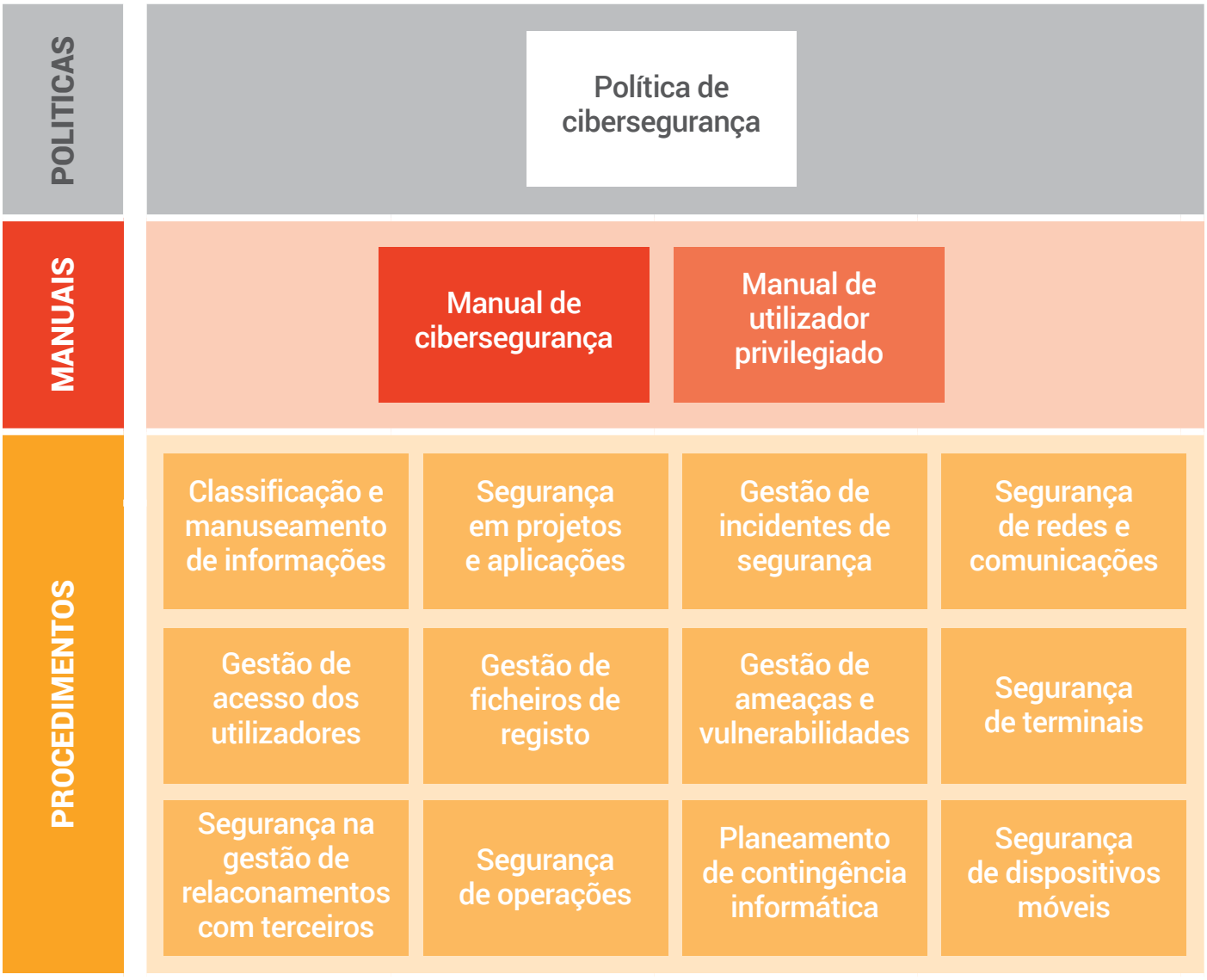
Todos os ficheiros de registo dos utilizadores (acesso, sistema, aplicações) são mantidos por um período de tempo em conformidade com a legislação local. Quando não existe legislação, este período é definido como 6 meses no mínimo e 1 ano no máximo.

ESTE MANUAL É PARTE INTEGRANTE DA ESTRUTURA DE CIBERSEGURANÇA DO GRUPO UNILABS.



10.REFERÊNCIAS

Este manual é parte integrante da Estrutura de Cibersegurança do Grupo Unilabs, que inclui os seguintes documentos chave:



APÊNDICE 1

Nota informativa a qualquer utilizador (colaboradores e terceiros autorizados, como funcionários não empregados, consultores ou contratados independentes, fornecedores ou clientes) que usam os recursos digitais da Unilabs.

SECÇÃO 1

Identidade e detalhes de contacto do controlador

De acordo com a legislação relevante de proteção de dados, os dados pessoais serão processados por:

Medicina Laboratorial - Doutor Carlos da Silva Torres, S.A.
Rua do Campo Alegre 231 5º Sala 7
4150-178 Porto

SECÇÃO 2

Objetivos do processamento e base legal

Os seus dados pessoais serão processados para os seguintes fins e de acordo com a base legal definida abaixo:

Objetivos	Base Legal
Gerir ativos de informática e telefones	Legitimar o interesse da Unilabs em fornecer ferramentas informáticas aos funcionários
Gerir incidentes informáticos	
Gerir mensagens e ferramentas de colaboração	
Gerir contas de utilizadores e autorizações	
Gerir redes e segurança	

SECÇÃO 3

Perfis

Não aplicável - sem perfis

SECÇÃO 4

Recolha indireta de dados

Não aplicável - sem recolha indireta de dados

SECÇÃO 5

Categorias de destinatários dos dados pessoais

Os seus dados pessoais serão partilhados com os seguintes destinatários:

- Dentro do Grupo Unilabs, incluindo outras empresas da Unilabs: com pessoal autorizado responsável pelo departamento de informática.
- Com prestadores de serviços que agem em nome da Unilabs e nos auxiliam na gestão das nossas atividades.

SECÇÃO 6

Período de retenção de dados

De acordo com a legislação de proteção de dados em vigor, os dados são retidos de acordo com a duração do contrato com a Unilabs e excluídos até 90 dias após o término do contrato.

SECÇÃO 7

Transferência de dados pessoais

Devido à dimensão internacional do Grupo Unilabs, os dados pessoais serão transferidos para fora da União Europeia, para países reconhecidos pela Comissão Europeia como garantia de um nível adequado de proteção, como a Suíça, onde se localiza a sede, e para outros países com diferentes níveis de proteção, como Austrália, Singapura, Brasil e Estados Unidos.

De acordo com o regulamento de proteção de dados, e para garantir a proteção dos seus dados pessoais, a Unilabs estabelece salvaguardas pertinentes, como a assinatura do contrato de transferência de dados com base nas cláusulas contratuais predefinidas emitidas pela Comissão Europeia. Por favor, escreva para o seguinte endereço se desejar obter cópias de tais contratos: **dpo@unilabs.com.**

SECÇÃO 8

Direitos dos titulares de dados

Em relação aos seus dados pessoais, os titulares têm os seguintes direitos:

- Direito de acesso, que podem exercer pedindo uma cópia dos seus dados pessoais;
- O direito de corrigir os seus dados pessoais, se estiverem imprecisos ou incompletos, e o direito de obter a restrição do processamento dos seus dados pessoais;
- O direito de eliminar os seus dados pessoais, se forem processados com base no seu consentimento, no desempenho de um contrato do qual é parte e nos nossos interesses legítimos;
- O direito à portabilidade de dados, se os seus dados pessoais forem processados com base no seu consentimento e/ou no desempenho de um contrato do qual é parte;
- O direito de se opor, por motivos relacionados à sua situação particular, ao processamento de seus dados pessoais nos casos em que são processados com base nos nossos interesses legítimos.

SECÇÃO 9

Meios de exercício

Os direitos podem ser exercidos enviando um e-mail no seguinte endereço: **dpo@unilabs.com**

SECÇÃO 10

Direito de apresentar uma queixa a uma APD

Tem também o direito de apresentar uma queixa a uma Autoridade de Protecção de Dados, quer no Estado-Membro da sua residência habitual, local de trabalho ou local de uma alegada violação do GDPR.

SECÇÃO 11

Dados de contacto do responsável pela protecção de dados

dpo@unilabs.com

APÊNDICE 1

Consentimento

Confirmo que li e compreendi o Manual de Cibersegurança da Unilabs.

Documento: Manual de Cibersegurança da Unilabs.
Versão 1
Distribuido em 07.03.2019

Primeiro Nome:

.....

Último Nome:

.....

Data:

.....

Assinatura:

.....

Distribuido em 07.03.2019
Versão 1

Unilabs