Política de Segurança da Informação

Grupo MEO

Índice

1. Introdução

A informação é um ativo crítico essencial para o negócio do Grupo MEO e, por esse mesmo motivo, necessita de proteção adequada. A proteção é especialmente importante num ambiente de negócio que está cada vez mais interligado. Como resultado do aumento da interligação, a informação está agora exposta a um número cada vez maior de diferentes vulnerabilidades e ameaças.

A Segurança da Informação e das Tecnologias de Informação e de Comunicação é assegurada através da implementação de um conjunto adequado de controlos que inclui políticas, processos, procedimentos, estruturas organizacionais, software e hardware. Estes controlos têm de ser estabelecidos, implementados, monitorizados, revistos e melhorados, sempre que necessário, para garantir que os objetivos específicos de segurança e empresariais do Grupo MEO são cumpridos.

A Política de Segurança da Informação do Grupo MEO contempla um capítulo relacionado com gestão dos riscos de ciber segurança da organização e gestão dos riscos de ciber segurança da cadeia de fornecedores.

O definido na presente Política prevalece sobre qualquer outro documento em vigor no Grupo MEO, (Política, Norma, Documento de trabalho, etc.).

2. Objetivos

A Política de Segurança da Informação visa estabelecer requisitos para garantir o nível apropriado de proteção da Informação do Grupo MEO ao nível de todos os Sistemas e Tecnologias de Informação e Comunicação, incluindo as plataformas de serviços de telecomunicações que suportam as suas operações e o seu negócio.

É política do Grupo MEO proibir acessos não autorizados, distribuição, duplicação, alteração, destruição ou apropriação indevida da informação das suas organizações, e proteger a informação de entidades externas, de forma consistente com o seu nível de classificação, em conformidade com todos os acordos, requisitos legais e normativos aplicáveis.

Além desta Política de Segurança da Informação existem para as áreas operacionais do Grupo MEO com especificidades tecnológicas relevantes, procedimentos complementares específicos de Segurança da Informação a serem seguidos.

A presente Política deve ser disponibilizada, a todos os colaboradores, fornecedores, parceiros, prestadores de serviço, entidades internas e externas que acedam à informação do Grupo MEO.

Para efeitos desta Política, é equiparada a informação do Grupo MEO, a informação de entidades externas que tenha sido confiada a empresas do Grupo MEO, ou à qual esta tenha acesso, ou que trate para quaisquer fins legais ou contratuais, exceto se expressamente ou do contexto resultar entendimento diferente.

3. Âmbito

A Política de Segurança da Informação aqui descrita é aplicável a:

a. Pessoas ou entidades, com acesso à Informação e aos Sistemas e Tecnologias da Informação e Comunicação do Grupo MEO, ou sob a responsabilidade desta, ou seja, colaboradores internos e externos, fornecedores, prestadores de serviços, parceiros, consultores, colaboradores de entidades externas e entidades internas com acesso à Informação e aos Sistemas e Tecnologias da Informação e Comunicação do Grupo MEO, ou sob a responsabilidade desta. O termo “Utilizadores” será utilizado genericamente em referência a qualquer um dos indivíduos ou entidades atrás referidas.

b. Pessoas ou entidades com responsabilidade direta ou indireta pela Arquitetura, Engenharia, Operação e Manutenção, incluindo evolução tecnológica, dos Sistemas e Tecnologias de Informação e Comunicação do Grupo MEO, ou sob a responsabilidade desta. Responsáveis pela garantia de que os diferentes Sistemas e Tecnologias da Informação e Comunicação são desenvolvidos e mantidos, no seu ciclo de vida, dentro dos requisitos de segurança definidos nesta Política. O termo "Responsável E&O" será utilizado genericamente em referência a qualquer um dos indivíduos ou entidades referidas neste ponto.

b. Entidades externas a quem as empresas do Grupo MEO adjudicam serviços, sempre que estas tenham acesso à Informação ou trabalhem diretamente sobre Sistemas e Tecnologias e Comunicação do Grupo MEO ou tenham sistemas ligados diretamente em rede1 com os Sistemas e Tecnologias e Comunicação do Grupo MEO.

b. Entidades externas a quem as empresas do Grupo MEO adjudicam serviços de tipologia "Cloud", nos modelos IaaS (infraestrutura como serviço), PaaS (plataforma como serviço), SaaS (software como serviço), etc. desde que haja dados do Grupo MEO armazenados.

Todos os Utilizadores e Responsáveis E&O, independentemente do seu nível hierárquico, função e vínculo contratual – internos do Grupo MEO ou afetos a entidades externas ou outros com quem as empresas do Grupo MEO contrataram um fornecimento de Produtos/Serviços – devem ter conhecimento desta Política e acesso adequado à informação necessária para o desempenho das suas funções, sendo exigido destes o respeito pelos controlos de segurança implementados, essenciais ao cumprimento sustentável dos seguintes valores mínimos da Segurança da Informação:

- **Integridade da informação** – prevenção contra a modificação e a destruição não autorizada de Informação, salvaguardando a respetiva fiabilidade e origem;
- **Confidencialidade da Informação** – prevenção contra o acesso e a divulgação não autorizados de Informação;
- **Disponibilidade da Informação** – garantia do acesso autorizado à Informação sempre e na medida do necessário.
- **Não-repúdio** – garantia que quem causou uma atividade ou evento não pode negar que a causou.
- **IAAAA** (Integridade, Autenticação, Autorização, *Auditing* e *Accounting*) – garantia da identificação (quem acede), autenticação (prova que foi quem acedeu), autorização (definição de permissões), auditing (registo de atividades e eventos em logs) e accounting (revisão dos logs para deteção de violações).

Deve igualmente ser assegurado que são guardadas evidências da divulgação a que se refere o parágrafo anterior.

A segurança da informação, ou seja, a sua confidencialidade, integridade, disponibilidade, não-repúdio e IAAAA, é uma responsabilidade de todos.

A Política aqui descrita é aplicável a todos os Sistemas e Tecnologias de Informação e Comunicação do MEO, bem como à comunicação entre estes. A aplicação desta Política deve, no entanto, ser efetuada de forma diferenciada de acordo com a seguinte classificação dos Sistemas e Tecnologias de Informação e Comunicação:

- Novos sistemas e tecnologias;
- Sistemas e tecnologias já existentes.

3.1 Aquisição de novos Sistemas e Tecnologias de Informação e Comunicação

Para os novos Sistemas e Tecnologias de Informação e Comunicação do Grupo MEO deve ser garantido o cumprimento integral da Política aqui definida, devendo este requisito ser assegurado desde o momento de procura e seleção da solução tecnológica a adotar (RFI, RFP, ...), logo durante a fase de

seleção e negociação com os possíveis fornecedores ou prestadores de serviços, pelo que aos mesmos deve ser disponibilizada, ao abrigo de cláusula de confidencialidade, nos termos dos parágrafos seguintes.

Na contratação de produtos e serviços, o Cliente interno deve salvaguardar que, a proposta apresentada pelo fornecedor refere expressamente, por escrito, que os produtos e serviços a serem contratados estão em conformidade com a Política de Segurança da Informação do Grupo MEO e que estão explicitamente refletidas nessa proposta as cláusulas de confidencialidade e proteção de dados pessoais constantes desta Política, sendo o fornecedor responsável pelos danos decorrentes para o Grupo MEO e terceiros pela violação da presente Política por parte do fornecedor e seus colaboradores, agentes e subcontratados.

O Cliente interno do MEO deve adicionalmente garantir, antes e após a adjudicação, que:

- A Arquitetura, o desenho, a implementação, integração, operação, manutenção e futura evolução da solução, incluindo eventuais ambientes de desenvolvimento, teste e controlo de qualidade, cumprem com a presente Política, bem como integram com todos os controlos de segurança oficiais da empresa, tais como as plataformas de Anti-DDoS, WAF's, Forward Proxies, mail relay's, etc;
- Todos os desenvolvimentos necessários de software, e de scripts de administração, têm por base as boas práticas de desenvolvimento de software, reconhecidas internacionalmente em matéria de segurança, de forma a evitar erros comuns e vulnerabilidades de segurança conhecidos;
- A Direção de *Cybersecurity* foi envolvida, sempre que o risco elevado, através do Procedimento Operativo Gestão de Exceções e Pareceres, publicado na plataforma de gestão documental do MEO, sendo cumpridos todos os requisitos de segurança que esta identificou, bem como são executados testes de segurança, adequados ao sistema/software em causa e acreditados ou validados pela Direção de Cybersecurity, para verificar a ausência de vulnerabilidades de segurança e outras não conformidades à presente Política;
- Qualquer fornecedor ou prestador de serviços envolvido na solução se compromete com as cláusulas de confidencialidade e segurança da informação estabelecidas nos contratos bem como com as demais cláusulas que garantem o cumprimento desta Política;
- Qualquer pessoa externa à MEO, que venha a ter acesso à solução, incluindo os ambientes de desenvolvimento, teste e de qualidade, assina uma Declaração de Confidencialidade que garanta o cumprimento desta Política para além de outras disposições específicas ao fornecimento em causa.

3.2 Sistemas e Tecnologias já existentes *(Legacy)*

Para os sistemas e tecnologias nestas condições, devem ser implementadas as alterações necessárias para garantir o cumprimento integral da Política aqui definida, exceto quando forem identificadas razões técnicas, de negócio ou de força maior que inviabilizem a implementação das alterações referidas, para as quais deve seguir-se o procedimento de gestão de exceções, de acordo com o descrito no capítulo 8 desta Política.

4. Responsabilidades Gerais

4.1 Responsabilidades da Gestão de Topo

É assumido o compromisso quanto à disponibilização dos recursos adequados necessários à execução da presente política, incluindo o pessoal, os recursos financeiros, os processos, as ferramentas e as tecnologias necessárias.

4.2 Responsabilidade do Responsável pela Segurança da Informação / Cibersegurança

Na dependência da Gestão de Topo, a organização dispõe de uma Direção responsável pelos temas da cibersegurança e segurança da informação.

4.3 Responsabilidades gerais dos Utilizadores

Os equipamentos informáticos disponibilizados pelo Grupo MEO aos Utilizadores destinam-se ao exercício da respetiva atividade profissional, devendo estes zelar pela sua boa conservação e utilização adequada. É da responsabilidade de cada Utilizador a salvaguarda da sua informação pessoal e garantir que esta não é ilegal, ilícita ou imprópria face ao código de ética do Grupo MEO. Os Utilizadores do Grupo MEO devem cumprir integralmente os termos e condições de utilização do software utilizado no âmbito das suas funções no Grupo MEO.

Um colaborador do Grupo MEO, enquanto Utilizador, que cometa uma violação à presente Política, ficará sujeito a sancionamento disciplinar, nos termos da Lei Geral de Trabalho e do Acordo de Empresa em vigor.

4.4 Responsabilidades gerais dos Administradores de Sistemas, Bases de Dados, Plataformas de Serviço, Equipamentos de Rede dos Sistemas e Tecnologias de Informação e Comunicação, Equipas Técnicas

Um colaborador do Grupo MEO, enquanto Utilizador, que tenha configurados acessos que lhe permitam administrar Sistemas, Bases de Dados, Plataformas de Serviço, Equipamentos de Rede dos Sistemas e das Tecnologias de Informação e Comunicação, é responsável:

- Pela salvaguarda da informação a que tem acesso, devendo garantir a confidencialidade da mesma, de acordo com a Declaração de Confidencialidade que obrigatoriamente tem de assinar.
- Por assegurar que os ativos sob sua administração técnica cumprem com esta Política. Garantindo, no mínimo, e condição necessária ao cumprimento desta Política, a aplicação das melhores práticas relativas à manutenção sustentada da ciber higiene2 dos ativos sob sua administração.

A chefia direta, destes colaboradores, é responsável por garantir que apenas os colaboradores com necessidade dos acessos privilegiados os têm configurados, devendo autorizar, rever e garantir a remoção dos mesmos, quando já não se justifiquem.

4.5 Responsabilidades gerais dos Responsáveis pela Engenharia, Operação e Manutenção dos Sistemas e das Tecnologias de Informação e Comunicação

Os Responsáveis pela Engenharia, Operação e Manutenção dos Sistemas e das Tecnologias de Informação e Comunicação (E&O), durante o ciclo de vida dos diferentes Sistemas e Tecnologias de Informação e Comunicação sob sua tutela, devem identificar, planear e obter aprovação / compromisso da gestão de topo de todas as condições, em termos de recursos financeiros e humanos, os processos e as ferramentas tecnológicas necessárias e as tecnologias de acordo com os ciclos de planeamento orçamental, que

permitam às respetivas equipas técnicas o cumprimento sustentado desta Política. No mínimo passará por evitar a obsolescência tecnológica e garantir a efetividade da aplicação das melhores práticas relativas à atualização contínua do software em termos de segurança (p.e., com a aplicação atempada de "patches" de segurança, atualização dos seus certificados digitais, atualização dos anti-virus quando for caso disso, erradicação de protocolos inseguros, ...).

4.6 Responsabilidades gerais das Entidades Externas

Os equipamentos informáticos disponibilizados pelo Grupo MEO a Utilizadores externos destinam-se à execução do serviço contratado, devendo estes zelar pela sua boa conservação e utilização adequada. É da responsabilidade de cada Utilizador a salvaguarda da sua informação pessoal e garantir que esta não é ilegal, ilícita ou imprópria face ao código de ética existente.

Estes Utilizadores devem cumprir integralmente os termos e condições de utilização do software utilizado no âmbito das atividades contratadas pelo Grupo MEO.

Caso se verifique uma violação da presente Política por parte de fornecedores, prestadores de serviços, parceiros e seus Utilizadores, o Grupo MEO poderá desencadear os meios legais ao seu alcance e aplicar as penalizações contratuais, bem como revogar imediatamente todos os direitos de acesso aos Sistemas e Tecnologias do Grupo MEO por parte do elemento incumpridor, devendo, para o efeito, ser alteradas as respetivas passwords de acesso aos sistemas e desativado o acesso às instalações do Grupo MEO.

4.7 Responsabilidades gerais das Chefias e das áreas de Gestão dos Recursos Humanos

Sempre que exista uma alteração de responsabilidades ou de funções de um Utilizador interno, a respetiva chefia deve de imediato desencadear a adequação dos privilégios de acesso desse Utilizador, aos diferentes Sistemas e Tecnologias de Informação do Grupo MEO. Se for Utilizador externo essa competência será do responsável da unidade interna onde o serviço é ou era prestado.

Sempre que um colaborador do Grupo MEO deixe de trabalhar na empresa, o sistema de gestão de acessos/identidades deverá espoletar automaticamente os pedidos de bloqueio aplicacionais devidos, ou a pedido dos responsáveis pelo colaborador, a equipa de gestão de acessos deve desativar todas as suas contas de acesso, com base em informação recebida pela área de Gestão de Recursos Humanos. Esta equipa desativa todos as contas de acesso a aplicações, bases de dados, sistemas operativos (que suportavam essas aplicações), redes wireless oficiais, sistemas RAS (Remote Access Service) e/ou VPN (Virtual Private Network), serviços Cloud, Hosting e Housing, e aos pontos de acesso físico aos edifícios da empresa. A área de Gestão de Recursos Humanos deve também garantir a recolha do cartão de empregado e de todos os meios informáticos a si disponibilizados pelo Grupo MEO (Desktop e/ou Notebook, telemóvel, ...).

Caso esse colaborador interno tenha, dentro das suas funções, lidado com informação confidencial ou com dados pessoais, toda a informação no seu Desktop e/ou Notebook deve ser destruída antes que este seja reaproveitado para outro Utilizador. Deve depois proceder à eliminação de toda a informação de caráter biométrico associado a esse colaborador e, finalmente, eliminar toda a informação residente nos discos internos ou "flash memory" dos dispositivos recolhidos, com exceção da que possa ser necessária para fins laborais.

Sempre que um colaborador de uma entidade externa deixe de desempenhar funções no Grupo MEO, a área na qual desenvolveu a sua atividade deve informar a equipa de gestão de acessos para que esta possa desativar todas as suas contas de acesso a aplicações, a sistemas operativos (que suportavam essas aplicações), a sistemas RAS (Remote Access Service) e/ou VPN (Virtual Private Network), bem como ao sistema de comunicação de voz (móvel e fixo) e aos pontos de acesso físico aos edifícios da empresa. A área interna responsável pelo serviço prestado pela entidade externa deve também assegurar a recolha de eventuais cartões de acesso assim como a eliminação de toda a informação de caráter biométrico associado a esse colaborador externo. Caso esse colaborador externo tenha, dentro das suas funções,

lidado com informação confidencial ou com dados pessoais, toda a informação no seu Desktop e/ou Notebook deve ser destruída antes que este seja reaproveitado para outro Utilizador.

É obrigatória a execução de um procedimento que reavalie periodicamente a necessidade da manutenção de contas em todos Sistemas, Bases de Dados, Plataformas de Serviço, Equipamentos de Rede dos Sistemas e das Tecnologias de Informação e Comunicação.

É responsabilidade do Grupo MEO a disponibilização do respetivo posto de trabalho (endpoint) aos colaboradores externos, não sendo permitido a utilização de postos de trabalho externos à rede do Grupo MEO, quer de forma remota (RAS ou VPN), quer localmente (pontos de rede local (LAN) e redes wireless dos edifícios da empresa). As exceções estão reguladas na Política Bring your own device do Grupo MEO.

5. Comunicação e Gestão da Informação

5.1 Classificação de informação

Os graus de classificação de segurança da informação, correspondentes ao nível de sensibilidade da informação, definidos na empresa são os seguintes:

- **Muito secreto** – Este grau de classificação Muito Secreto é limitado a informações, documentos e materiais que necessitem do mais elevado grau de proteção. Deve ser aplicado unicamente a matérias cujo conhecimento ou divulgação por pessoas não autorizadas para tal, possa implicar consequências excecionalmente graves para o Grupo MEO ou para uma das suas Empresas participadas.

  São exemplos de matérias a classificar de Muito Secreto as que constem de diretivas, planos ou ordens estratégicas ao nível de administração das empresas.

  A atribuição do grau de classificação Muito Secreto compete exclusivamente aos membros da Comissão Executiva ou equivalente, não podendo em caso algum ser subdelegada.

- **Secreto** – Este grau de classificação aplica-se a matérias cujo conhecimento ou divulgação por pessoas não autorizadas para tal, possa implicar consequências graves para o MEO ou para uma das suas Empresas participadas.

  São exemplos de matérias a classificar de Secreto as que constem de estudos e documentos sobre o fornecimento de novas soluções tecnológicas ou aperfeiçoamentos considerados estratégicos para o negócio, ou outras circunstâncias que denunciem questões altamente sensíveis para o MEO. Nesta classificação, é ainda enquadrável informação técnica como p.e., passwords de sistemas críticos do MEO.

  A atribuição do grau de classificação Secreto compete aos membros do Comité Executivo ou equivalente, ou ainda aos Diretores das Empresas.

- **Confidencial** – Este grau de classificação aplica-se a matérias cujo conhecimento ou divulgação por pessoas não autorizadas para tal, pode ser prejudicial para o MEO ou para uma das suas Empresas participadas..

  São exemplos de matérias a classificar como Confidencial:

  - Documentos ou informação operacional, técnica ou comercial que possam conter informação útil à concorrência;
  - Informações ou estudos sobre grandes clientes ou segmentos de mercado que possam conter informação útil à concorrência;
  - Ficheiros com dados pessoais de clientes ou de outras pessoas singulares;
  - Toda a informação proprietária de clientes;

- Processos de natureza laboral ou disciplinar;
- Informação privada referente a colaboradores internos e externos.

- **Reservado** – Este grau de classificação é aplicado a matérias limitadas ao uso departamental que, embora não requerendo classificação mais elevada, não devem ser do conhecimento de pessoas que delas não necessitem para o estrito cumprimento das suas funções.

  São exemplos de matérias a classificar como Reservado:

  - Textos técnicos cujo conteúdo exija proteção no interesse das Empresas;
  - Informação de firmas ou organizações, relativas a ofertas, propostas ou transações cujo conhecimento indevido possa prejudicar ou favorecer indevidamente terceiros.

  Qualquer informação da empresa não classificada explicitamente com um grau de classificação é classificada por omissão com grau Reservado.

- **Público** – Este grau de classificação é aplicado a matérias que se destinem explicitamente ao domínio público.

No âmbito desta Política, sempre que seja mencionado "Informação Classificada", referese a informação classificada, não classificada como Pública.

A atribuição dos graus de segurança Reservado e Confidencial compete aos colaboradores que assinam o documento ou informação cuja segurança se desejam garantir, tendo em consideração as regras e a necessidade atrás definidas. Esta informação não deve ser reencaminhada a não ser que tal seja necessário e crítico para o negócio, e neste caso a mensagem e respetivos anexos têm de estar cifrados.

A informação classificada como Muito Secreto, Secreto ou Confidencial, armazenada em bases de dados ou ficheiros do sistema, fixos ou amovíveis, devem ser cifrados de acordo com a Norma Técnica de Criptografia e PKI, publicado na plataforma de gestão documental do Grupo MEO, de forma a evitar a leitura não autorizada, mesmo por quem tenha privilégios máximos de administração de sistemas ou bases de dados ou por um eventual hacker.

Equipamentos com acesso a informação classificada como Muito Secreto e Secreto devem, sempre que possível, utilizar filtro de privacidade.

As instalações do Grupo MEO nas quais esteja armazenada informação classificada como Muito Secreto e Secreto devem assegurar mecanismos de controlo de entrada (cartões de identificação, restrição de acesso aos pisos, deteção de impressão digital por via ótica ou outros meios biométricos), de forma a identificar, autenticar e registar as entradas e deslocações.

A informação que entra no Grupo MEO deve manter a classificação atribuída pelo fornecedor / parceiro / prestador de serviço, etc, e devem ser garantidos os controlos de segurança de proteção da informação aceites / acordados entre as partes. A informação não classificada segue o princípio definido para a informação interna da organização, logo é classificada por omissão como reservada.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, control, 5.12 Classification of information, 8.12 Data leakage prevention.

5.2 Gestão de Meios Amovíveis

5.2.1 Utilização de Meios Amovíveis

As drives para meios amovíveis (USBs, Discos externos, DVD's, Tapes, etc.), não devem estar disponíveis nas Estações de Trabalho (ET) se não houver uma razão de negócio que o justifique.

Cabe ao Diretor de cada área a identificação e autorização das ET para as quais devem ser disponibilizadas as drives para os meios amovíveis. Deve, no entanto, ser garantido que não são disponibilizadas ou permitidas drives para meios amovíveis no caso das ET de risco (ver 6.5.2).

É estritamente proibida a execução de software não autorizado a partir de qualquer meio amovível.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, control, 7.10 Storage media.

5.2.2 Transporte da Informação Classificada

Sempre que seja necessário efetuar o transporte de um qualquer meio amovível ("USB pens", Discos externos, CDs, DVD's, Tapes, etc.) com informação classificada devem ser garantidas todas as medidas necessárias, antes, durante, e depois do transporte, para proteger a confidencialidade, integridade e disponibilidade da Informação. A informação contida nos meios amovíveis a utilizar deve ser cifrada previamente ao transporte.

O transporte de informação classificada deve ser feito por Utilizadores autorizados para o efeito.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, control 7.10 Storage media

5.3 Eliminação da Informação

5.3.1 Eliminação de Documentos Classificados

Devem ser destruídos periodicamente, e logo que conveniente, todos os documentos já substituídos ou caducados, salvo no caso de matérias classificadas como Muito Secreto em relação às quais a destruição apenas será feita após solicitação ao arquivo pela entidade emissora.

Sempre que o detentor de matéria ou documento classificado de Muito Secreto entenda que o mesmo se tornou inútil deve propor à entidade emissora que proceda ou mande proceder à sua destruição. Os serviços responsáveis pelo arquivo de matérias classificadas não necessitam de aguardar instruções para procederem à destruição de rotina de documentos classificados. Em regra, deve evitar-se a manutenção em arquivo de documentos classificados com mais de 5 anos, cujo interesse histórico não seja reconhecido, ou que se tenham tornado desnecessários. Na destruição de rotina de documentos classificados, devem ser usadas máquinas trituradoras, retalhadores ou incineradores que garantam eficazmente a inutilização efetiva da informação neles contidos.

Deve ser sempre considerado o tempo de retenção definido para cada tipo de informação antes de avançar com a sua eliminação, verificando-se, para o efeito, o período de conservação legalmente exigido, designadamente em matéria fiscal, contabilística ou em conformidade com os Registos de Atividades de Tratamento, de acordo com as finalidades definidas pelo responsável pelo tratamento, nos termos do Regulamento Geral de Proteção de Dados (RGPD).

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, control, 5.33 Protection of records, 8.10 Information deletion.

5.3.2 Eliminação de Media

Todos os CDs/DVD's, discos magnéticos, bandas/cartridges magnéticas, etc. que já não sejam necessários devem ser fisicamente destruídos ou colocados em recipientes adequados para que sejam posteriormente destruídos por uma empresa devidamente certificada para o efeito. O processo de destruição física deve impossibilitar qualquer recuperação de informação mesmo que parcial. Esta destruição deve ser sempre realizada por uma empresa cuja relação contratual assegure a necessária confidencialidade.

Sempre que termine a colaboração de um colaborador (interno ou de uma entidade externa) a respetiva chefia ou o responsável pela área na qual desenvolveu a sua atividade deve informar a área responsável pela Gestão de Equipamentos visando a eliminação adequada dos registos de informação do colaborador, garantindo a confidencialidade da informação relativa à função desempenhada.

É da responsabilidade do Colaborador (interno ou de uma entidade externa) com o qual terminou a colaboração a salvaguarda da sua informação pessoal, não assumindo o Grupo MEO qualquer responsabilidade relativamente a essa informação pessoal.

Devem ser estritamente garantidos os prazos de retenção para os diferentes tipos de informação de acordo com as diferentes leis a que o Grupo MEO está obrigado.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, control, 7.10 Storage media, 8.10 Information deletion

5.4 Armazenamento da Informação

5.4.1 Armazenamento da Informação em Servidores

Todos os servidores com informação relevante do Grupo MEO têm de estar alojados em Data Center ou salas técnicas do tipo ANG (Áreas de Nova Geração) sob a responsabilidade de uma entidade operacional reconhecida que assegure a administração de sistemas e a sua segurança física e lógica dentro das melhores práticas e do disposto na presente Política.

Os servidores com informação classificada acima de Reservado do Grupo MEO, dos diversos ambientes, nomeadamente, desenvolvimento, laboratórios, testes e produtivo, devem estar devidamente identificados na CMDB e refletir o correto estado de operacional (p.e. produtivo/ abate/ desligado/ etc), de forma a gerar automaticamente alertas para as equipas responsáveis.

Sempre que um servidor deixe de ser utilizado deve ser imediatamente desligado da rede e a sua informação destruída após verificação do período de conservação do tipo de dados, nos termos previstos na lei aplicável, designadamente em matéria contabilística e fiscal e nos registos de Tratamento de Dados Pessoais, enquadrado nas Finalidades/Tratamentos de Dados definidas no RGPD. No caso excecional em que este servidor tenha de ser mantido mais algum tempo ligado à rede interna, será obrigatório garantir a sua segurança lógica através da eliminação de todos os acessos lógicos desnecessários para impedir a utilização maliciosa.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, control, 7.8 Equipment siting and protection.

5.4.2 Armazenamento da informação necessária à gestão e administração técnica de Sistemas, Bases de Dados, Plataformas de Serviço, Equipamentos de Rede dos Sistemas e das Tecnologias de Informação e Comunicação

A informação necessária à gestão e administração técnica de Sistemas, Bases de Dados, Plataformas de Serviço, Equipamentos de Rede dos Sistemas e das Tecnologias de Informação e Comunicação, p.e. registo de passwords, certificados, chaves, etc., deve ser armazenada num sistema que garanta o controlo

de acessos à mesma, nomeadamente do tipo “Password Vault Management ” e “Certificate Management”

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, control, 5.37 Documented operation procedures

5.4.3 Gestão e Utilização da Documentação de Sistemas e Tecnologias de Informação

A documentação relativa aos Sistemas e Tecnologias de Informação e Comunicação do MEO (p.e., manuais operacionais e de utilização) deve estar atualizada e acessível apenas a quem for autorizado.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, control, 5.37 Documented operation procedures.

5.5 Comunicação de Informação

5.5.1 Comunicação de Informação Classificada

Não é permitida a transmissão, por meios eletrónicos de qualquer tipo (incluindo e-mail, fax, telefone, telemóvel e Internet), de matéria ou documento classificado como Muito Secreto ou Secreto, ainda que parcial.

Informação classificada como Confidencial ou Reservado não poderá ser enviada para uma impressora de rede sem que alguém autorizado salvaguarde a confidencialidade durante a impressão e recolha do documento, e não deve ser reencaminhada para fora da empresa a não ser que seja necessário e crítico para o negócio do Grupo MEO, e nesse caso os dados devem ser cifrados antes de envio. Sempre que possível, a transmissão de credenciais, deve ser efetuada separadamente e por diferentes canais de comunicação, caso contrário o risco deve ser avaliado pela área de Cibersegurança de acordo com o ponto 8 esta Política.

Ao enviar para destruição e posterior reciclagem documentos desta natureza deve ser assegurado que o resultado é ilegível.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.14 Information transfer.

5.5.2 Utilização de Computadores Portáteis e de outros Dispositivos Móveis (tablets, smartphones, ...)

Colaboradores que utilizem computadores portáteis do Grupo MEO não devem deixar o equipamento sem o respetivo cadeado. A proteção de documentos por password usualmente disponibilizada em algumas aplicações (p.e., Microsoft Word, Microsoft Excel, Adobe), não é suficiente.

Os dispositivos móveis podem ser roubados ou extraviados, podendo estar mais sujeitos à interceção de dados e informação, sendo por isso necessários controlos de Segurança da Informação adicionais no caso em que tenham de aceder a informação classificada do Grupo MEO.

Para cada tipo de dispositivo móvel que tenha de aceder a informação classificada do Grupo MEO devem ser assegurados os seguintes controlos de Segurança da Informação: proteção física, controlos de acesso, encriptação de informação armazenada e transferida, cópia de segurança de dados, proteção contra vírus, malware e intrusões.

Em caso de perda ou roubo deve ser acionado o procedimento constante no sistema de suporte ao Utilizador em vigor na empresa (p.e., OneDesk).

O Grupo MEO dispõe de um Política interna de Bring Your One Divice (BYOD), onde estão claramente definidas as diretrizes para a utilização dos mesmos, em que circunstâncias, quando, e quem pode aprovar a sua utilização.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.33 Protection of records, 8.1 User end point devices

.

5.5.3 Política e Princípios de utilização do e-mail

Qualquer mensagem enviada de um domínio de e-mail do Grupo MEO ou com assinatura contendo referência a empresas do Grupo MEO (mesmo que enviada de um domínio de e-mail pessoal de um colaborador) poderá ser considerada pelo "público em geral" como uma afirmação/posicionamento oficial da organização. Neste sentido o e-mail da organização não poderá ser utilizado para a criação e distribuição de qualquer mensagem contrária à lei e ao disposto no código de ética do Grupo MEO.

Só poderão ser enviadas mensagens por um domínio e/ou subdomínio de e-mail do Grupo MEO, pelos servidores que sejam devidamente autorizados, legitimados e com políticas definidas, utilizando para o efeito os standards de segurança SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) e DMARK (Domain-based Message Authentication Reporting and Conformance).

É aceitável que os colaboradores do Grupo MEO utilizem para fins pessoais o sistema de e-mail da organização, desde que tal uso seja devidamente moderado, não viole o código de conduta do Grupo MEO e respeite as regras estabelecidas nesta Política, bem como noutros instrumentos do Grupo MEO sobre este tema.

A utilização do sistema de e-mail do Grupo MEO está sujeita aos controlos de segurança necessários ao combate ao SPAM, PHISHING, SPEARPHISHING e a infeções por Vírus e outro Malware. O sistema de logging dos e-mails enviados e recebidos, e dos atos de administração relativos às diferentes mailboxes, segue todos os requisitos da salvaguarda da privacidade dos utilizadores e das obrigações previstas na lei.

5.5.3.1 Sistemas autorizados

Apenas é permitido o envio de e-mails pelas aplicações (e-mail clients) instaladas nas ET ou sistemas devidamente autorizados, não podendo ser reencaminhados de forma automática para e-mails externos ao Grupo MEO.

Sempre que se justifique devem ser utilizados Certificados Digitais para a assinatura e cifra dos e-mails.

5.5.3.2 Uso indevido

- Envio de chain letters de um e-mail do MEO;
- Envio de e-mails massivos, (p.e., para uma lista de distribuição de grande dimensão), exceto se efetuado por órgãos autorizados do Grupo MEO;
- Criação de e-mails fazendo-se passar por terceiros é uma violação desta Política e poderá dar origem a procedimento disciplinar e judicial.

5.5.3.3 Atuação em caso de suspeita

Os Utilizadores nunca devem abrir documentos, ficheiros, macros, ou URL's (links) que recebam em anexo de um e-mail cuja origem seja desconhecida, ou haja suspeita de que o conteúdo possa ser prejudicial, indicie o roubo de password ou de usurpação de identidade.

O Utilizador deve reportar de imediato (anexando os documentos ou e-mails) pelo sistema de suporte ao Utilizador em vigor e eliminar imediatamente os mesmos. Posteriormente deve esvaziar a pasta “Itens Eliminados”.

Todos os e-mails de Spam, chain letters, e semelhantes devem ser imediatamente eliminados (inclusive da pasta de “Itens Eliminados”) e nunca devem ser reenviados.

De forma a garantir a segurança e desempenho dos sistemas, podem ser realizadas tarefas de controlo de e-mails de forma aleatória e filtragens de certos ficheiros incluídos em e-mails, nomeadamente os afetados por vírus informáticos ou aqueles, que pelo seu formato (p.e., .exe, .bmp), possam representar um potencial perigo para a integridade dos sistemas e tecnologias de informação e comunicações.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 5.14 Information transfer

5.5.4 Utilização de Serviços de Messaging com encriptação end- to-end

Qualquer mensagem enviada por um Serviço de Messaging com assinatura contendo referência a empresas do Grupo MEO (mesmo que enviada de um utilizador pessoal de um colaborador interno ou externo) poderá ser considerada pelo “público em geral” como uma afirmação/posicionamento oficial da organização. Neste sentido o Serviço de Messaging não poderá ser utilizado para a criação e distribuição de qualquer mensagem contrária à lei e ao disposto no código de ética do Grupo MEO.

É permitida a utilização de Serviços de Messaging desde que seja garantida a encriptação end-to-end (WhatsApp, Signal, Telegram, etc).

Estes meios de comunicação devem ser utilizados como meio complementar aos meios existentes no Grupo MEO, nomeadamente, e-mail corporativo, serviços de messaging corporativo (Microsoft Teams, Microsoft Lync/ Skype for Business, etc.).

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 5.14 Information transfer.

5.5.5 Desenvolvimento de Sistemas – Utilização de Criptografia na Comunicação

Devem ser utilizados os algoritmos standard e não proprietários, aceites pela comunidade de cibersegurança como sendo estado da arte, e que se encontram descritos na Norma Técnica Interna de Criptografia e PKI do Grupo MEO. Os requisitos da dimensão da chave de cifra são revistos e atualizados de acordo com as evoluções tecnológicas. Não é permitida a utilização de algoritmos de cifra proprietários.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 8.24 Use of cryptography.

5.5.6 Comunicação de informação entre sistemas e aplicações

Sempre que informação sensível ou classificada tenha de circular entre duas aplicações ou sistemas fora de um perímetro seguro devem ser obrigatoriamente utilizados Protocolos Seguros (p.e., HTTPS, SSL/TLS, SSH ou IPSec). No caso de não ser possível segregar a informação classificada de diferentes níveis, deve adotar-se todas as medidas de segurança da classificação mais elevada.

Sempre que se realizem novas aquisições de sistemas ou aplicações, deve garantir-se que todos suportam Protocolos Seguros de comunicação e de administração.

Excecionalmente, o protocolo FTP pode ser usado nos sistemas legados que tenham de transferir informação classificada e que, por razões técnicas históricas, não suportem versões seguras de transferência de ficheiros (p.e., SFTP ou SCP). Nestes casos, o acesso deve:

- Ser apenas permitido entre os equipamentos que destes serviços necessitem, devendo o acesso estar bloqueado para todo e qualquer outro IP. Violações a este ponto devem constituir eventos monitorizados pelo Security Operations Center (SOC) do Grupo MEO;
- Ser efetuado sempre que possível através do Entreposto de Ficheiros;
- Estar cadastrado na respetiva CMDB (Configuration Management Database), ou equivalente, para controlo periódico.

Relativamente aos Sistemas e Tecnologias legados que, por razões técnicas, não possam cumprir integralmente o disposto, todas as exceções devem ser documentadas, num cadastro oficial de ativos (p.e., CMDB), devendo garantir a confidencialidade das mesmas e que o acesso às mesmas é efetuado apenas por Utilizadores autorizados.

Sempre que uma ação de renovação tecnológica não conduza ao cumprimento integral desta Política deve ser mantida a identificação deste sistema como uma exceção documentada.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 5.14 Information transfer, 8.24 Use of Cryptography.

5.5.7 Garantia de Segurança nos Front-Ends Internet/Extranet/Intranet

Para as soluções Internet e Extranet do Grupo MEO deve, obrigatoriamente, ser utilizado o protocolo https nas zonas da aplicação que envolvam informação classificada, o protocolo http é usado apenas nas situações em que toda a informação seja classificada como Público.

Embora nesta versão da presente Política a obrigação do protocolo https apenas está restrito às zonas envolvendo informação classificada, em próximas versões essa restrição passará a universal e os principais browsers a isso obrigarão, pelo que, por omissão, o protocolo https deve ser sempre utilizado em todas a novas implementações de sistemas e tecnologia.

Em qualquer das circunstâncias, os front-ends Web das soluções atrás referidas devem estar sempre protegidos num Data Center do Grupo MEO dentro de uma DMZ segura, com interfaces internas (da DMZ para os backends) e externas (da DMZ para a rede onde estão os Utilizadores) devidamente protegidas e monitorizadas pelo Security Operations Center (SOC) do Grupo MEO. Deve ser garantida a segregação de DMZ´s internas e externas. Se a solução for crítica para o Grupo MEO deve garantir-se adicionalmente, múltiplos front-ends Web distintos (no mínimo 2), em cluster, divididos por infraestruturas físicas diferentes, e devidamente balanceados por um load balancer ou arquitetura equivalente com capacidade adequada.

Desta forma assegura-se:

- Melhor gestão dos recursos, por permitir escalabilidade;
- Menor exposição de portos IP à Extranet ou Internet, permitindo consolidar os acessos vindos do exterior e facilitar a monitorização dos mesmos pelo Security Operations Center (SOC);
- Maior simplificação na configuração e gestão dos dispositivos de segurança da DMZ monitorizados pelo SOC;
- Prevenção e mitigação de eventuais ataques DoS (Denial of Service) à entrada do load balancer, poupando os servidores a ele conectados;
- Implementação de endereçamento virtual impedindo dessa forma que seja conhecido e acedido diretamente do exterior. diretamente do exterior.

Deverão ser garantidos mecanismos de proteção de cibersegurança para sistemas expostos à internet ou extranets, cuja informação seja considerada crítica, nomeadamente abrangidas pelo RGPD e demais legislação, regulamentemos aplicáveis à atividade do Grupo MEO, nomeadamente soluções de anti DoS e WAF (Web Application Firewall).

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.21 Security of network services.

5.6 Política e Princípios de "Clear desk and clear screen "

O MEO comprometida com a melhoria progressiva das suas práticas de segurança da informação define abaixo os princípios básicos de "Clear desk and clear screen" ("mesa limpa"):

- Que visam garantir o correto armazenamento, salvaguarda da informação nos seus diferentes suportes, nomeadamente, físicos e lógicos com informação do MEO;
- Pretendem estabelecer os requisitos básicos para que o espaço de ambiente se mantenha limpo e arrumado, onde as informações e materiais com informação da empresa estão protegidas, nomeadamente sobre funcionários, clientes, fornecedores e propriedade intelectual do MEO;
- Aplicam-se a todas as Pessoas ou Entidades, com acesso à Informação e aos Sistemas e Tecnologias da Informação e Comunicação do MEO, ou sob a responsabilidade desta, quer sejam colaboradores internos, colaboradores externos, fornecedores, prestadores de serviços, parceiros e consultores.

Em cumprimento das mesmas devem de ser observados os seguintes princípios específicos:

1. As Pessoas ou Entidades têm de proteger todas as informações do MEO, quer físicas quer lógicas, presentes no seu ambiente de trabalho;
2. Sempre que se ausentar do seu posto de trabalho, e para evitar o acesso à informação contida na sua estação de trabalho, o colaborador deve:
    a. Bloquear o ecrã, podendo para tal utilizar a sequência de comandos: "Ctrl-Alt-Del"+"Lock this Computer" ou tecla Window + L;
    b. Desligar a sua estação de trabalho quando se ausenta ao fim do dia de trabalho ou fazer "log off", sempre que se aplicar;
    c. Deixar o cadeado colocado no laptop ou guardá-lo em armário trancado.
3. Dispositivos de armazenamento em massa autorizados devem ser considerados material sensível, pelo que deverão de ser armazenados em local protegido/ trancado sempre que não se encontrem em utilização;
4. As impressoras devem ter controlo de acesso lógico (p.e. Copy Points do MEO). Caso não seja possível a implementação de tal controlo as mesmas devem estar localizadas em espaços reservados e com controlo de acesso físico;
5. A impressão de documentos deverá ser evitada, devendo dar-se primazia à partilha e gestão de documentos de forma eletrónica e segura. Cópias impressas deverão ser recolhidas imediatamente das impressoras após a sua impressão; Documentos em suporte físico, quando não estiverem em uso, não devem ser deixados sobre a secretária, fax, impressora ou fotocopiadora nem em qualquer outra área do ambiente de trabalho;
6. A destruição de documentos e informação classificada deve observar o definido no ponto 5.3.1;
7. As passwords devem seguir as diretrizes definidas na Política de Segurança da Informação do MEO e não devem ser anotadas ou armazenadas em nenhum suporte físico (p.e. Post-its, etc.);
8. Chaves e cartões de acesso não devem ser deixados sem vigilância;
9. Os quadros de reuniões e flip charts devem ficar limpos após a sua utilização;
10. Colaboradores internos, colaboradores externos, fornecedores, prestadores de serviços, parceiros e consultores não deverão verbalizar informação confidencial em "open spaces" ou em qualquer

espaço público, devendo utilizar espaços reservados, sempre que seja necessário ter uma conferência telefónica ou de vídeo, garantindo convocatória/ presença apenas das Pessoas ou Entidades que devem ter acesso a essa informação;

11. Todos os Princípios anteriormente referidos aplicam-se igualmente quando as Pessoas ou Entidades estejam em regime de Teletrabalho ou quando acedam remotamente à rede do MEO ou manuseiem informação do MEO.

É responsabilidade de cada um garantir a aplicação deste Princípios de "Clear desk and clear screen" do MEO. Violações repetidas ou graves dos mesmos poderão despoletar ações disciplinares bem como procedimento legal, civil ou criminal.

Caso algum dos seus dispositivos e/ou documentos se encontre em falta, ou se acredita que a sua área de trabalho foi violada, os colaboradores (internos ou externos) devem reportar esta situação imediatamente, de acordo com o Ponto 9. Comunicação de Incidentes de Segurança da Política de Segurança da Informação do MEO.

Exceções ao presente documento devem ser avaliadas, em termos de risco, pela Direção de Cybersecurity, de acordo com o Ponto 8 (Exceções e Pareceres à Política de Segurança da Informação) da Política de Segurança da Informação do MEO.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 7.7 Clear desk and clear screen.

6 Gestão de Acessos

6.1 Gestão de Acessos de Utilizadores

O MEO deve adotar, transversalmente, um sistema de gestão de identidades centralizado.

Nesse sistema devem estar armazenados os dados que identificam todos os Utilizadores, internos e externos, definindo os seus privilégios de acesso aos diferentes sistemas, tecnologias e aplicações, o período de validade de cada um desses privilégios e a cadeia de autorização.

A atribuição de acessos deve seguir o princípio RBAC (Role Based Access Control) que tem como base as funções e tarefas que os utilizadores desempenham na Organização.

De forma a garantir um nível de segurança adequado, as seguintes regras devem ser implementadas:

- Todos os sistemas, tecnologias e aplicações devem permitir autenticar e validar os privilégios de acesso de cada um dos seus Utilizadores;
- Acessos a sistemas, tecnologias e aplicações devem ser via autenticação por user/password, que deve ser única para cada Utilizador individual, ou por mecanismos de autenticação mais forte, entretanto adotados pelo MEO e aprovados pela Direção de Cybersecurity (DCY). Não é permitida a partilha de mecanismos de autenticação por grupos de Utilizadores.
- Contas com perfil de acesso privilegiado, nomeadamente de Administração da AD e de Domínios, de Administração de Sistemas, de Bases de Dados, de Plataformas de Serviço, de Equipamentos de Rede dos Sistemas e das Tecnologias de Informação e Comunicação, devem utilizar a autorização do acesso utilizando adicionalmente um mecanismo de two factor authentication (2FA) ou de multifactor authentication (MFA).
- Nas funções de administração mais críticas, como, por exemplo, as de "AD & Domain Admin" e de Administração dos Sistemas de Backup, para além do 2FA/MFA, deve ser usada uma solução de "Privileged Account Security" (PAS), como, por exemplo CyberArk.

- Todos os sistemas de acesso à rede interna do MEO a partir da Internet (por exemplo, VPN e CITRIX) deverão exigir 2FA/MFA para todos os utilizadores com funções de administração de sistemas, com perfis de acesso não limitados em termos do que podem aceder ou perfis nominais aplicacionais críticos com possibilidade de efetuar transações ou funções com impacto significativo.
- Adicionalmente, deve ser utilizado este mecanismo de 2FA ou MFA sempre que se justifique face à criticidade do ativo acedido.
- Qualquer situação que necessite de análise específica deverá ser observado o Ponto 8 (Exceções e Pareceres à Política de Segurança da Informação) da presente Política.
- Sempre que possível, a interface apresentada para autenticação deve incluir o seguinte alerta:

  "Este sistema apenas deverá ser usado por Utilizadores autorizados. Ao continuar a usar este sistema o Utilizador reconhece que é um Utilizador autorizado, reconhece que as utilizações deste sistema são registadas e compreende que as violações a esta Política poderão despoletar ações disciplinares bem como procedimento legal civil ou criminal".
- É proibido qualquer acesso anónimo aos sistemas ou aplicações do MEO (p.e., através de Utilizadores Guest). Estas contas devem estar todas desativadas.
- Pedidos de novos Utilizadores ou de alteração de privilégios devem passar por um processo de validação que inclua a área de Recursos Humanos, no caso dos internos e das áreas responsáveis pela contratação, no caso dos externos, devendo ser efetuados por escrito, utilizando templates pré-definidos ou aplicações informáticas específicas para o efeito e aprovados pela respetiva chefia antes de implementados.
- Todos os Utilizadores inativos durante 60 dias (máximo) deverão ser automaticamente bloqueados; Utilizadores inativos durante 1 ano (máximo) deverão, se possível tecnicamente e sem impacto na rastreabilidade dos Utilizadores, ser automaticamente removidos, caso contrário deverão ser mantidos bloqueados;
- Privilégios atribuídos a Utilizadores externos à organização deverão expirar automaticamente, no máximo, ao fim de 90 dias. Exceções a esta regra poderão ser implementadas, desde que sejam identificadas pelo respetivo interlocutor autorizado do MEO, que definirá o prazo adequado para o respetivo acesso. Sempre que seja necessário prolongar este período deverá ser autorizado novo pedido, pela mesma entidade;
- Sempre que exista uma alteração de responsabilidades ou funções de um Utilizado a respetiva chefia deve solicitar a correspondente adequação das contas de acesso do Utilizador.
- Para sistemas e aplicações críticas, é imperativa a execução de um procedimento que obrigue periodicamente à revalidação, por parte dos responsáveis hierárquicos, a necessidade da manutenção do acesso aos Utilizadores, essa revalidação deverá acontecer no mínimo com uma periodicidade anual para cada utilizador.
- Sempre que um técnico com acessos ativos a contas de administração de qualquer equipamento, cesse funções é obrigatória a suspensão de todas as suas contas nesses sistemas ou equipamentos. É obrigatória a execução de um procedimento que reavalie periodicamente a necessidade da manutenção de contas com privilégios de administração em todas as tecnologias, sistemas e aplicações, quer sejam de informação (BSS ou OSS) ou de comunicação.
- Todos os colaboradores com acesso a contas de administração de sistemas/ tecnologias/ aplicações devem estar cobertos por Declaração de Confidencialidade ou disposição contratual ou legalmente equivalente.
- A concessão de acessos deve respeitar o princípio "need to know", ou seja, os acessos devem ser facultados com base nas necessidades funcionais de cada colaborador.
- Sempre que possível a concessão de acessos deve assegurar a segregação de funções dos Utilizadores de desenvolvimento, teste e produção. Os Utilizadores da equipa de desenvolvimento não devem ter privilégios de acesso de escrita ao ambiente de produção.
- Se um Utilizador, que não faça parte da área técnica de Operação, Gestão e Manutenção, de Sistemas, das Aplicações, das Base de Dados, etc., e no âmbito das suas funções necessitar de acesso aos mesmos, com privilégios de Administração, deve apresentar a respetiva justificação e aprovação da

chefia direta e tal ficar devidamente documentado na CMDB ou aplicação utilizada para a gestão de contas e perfis.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.16. Identity management, 5.18 Access rights, 8.12 Data leakage prevention.

6.2 Política de Passwords de Utilizadores

Todos os Utilizadores devem ter a sua própria password de acesso aos sistemas informáticos do MEO, sendo esta password pessoal e intransmissível. As passwords são utilizadas para as mais diversas finalidades: contas de acesso a aplicações, contas de administração de sistemas, contas de plataformas de serviço, contas de administração de equipamentos de rede, contas web, contas de e-mail, proteções screen saver, proteções do voice mail, etc. Nesse sentido devem ser implementadas as seguintes regras:

- Após a instalação de qualquer aplicação/sistema/tecnologia deve garantir-se que todas as passwords de fábrica (atribuídas por omissão pelos fornecedores) de contas com privilégios de administração são alteradas de acordo com as regras definidas nesta Política de Segurança; de igual forma todas as contas de Guest ou outras não necessárias ao funcionamento do MEO devem ser imediatamente inibidas;
- As passwords atribuídas por omissão a novos Utilizadores de aplicações/ sistemas/ tecnologias devem cumprir as regras de robustez definidas nesta Política e ser obrigatoriamente alteradas após o primeiro logon. Se a password não for alterada a validade dos novos Utilizadores é de 48 horas, período após o qual a conta deve ficar bloqueada;
- De forma a prevenir possíveis ataques à segurança da informação, o número de tentativas consecutivas para autenticação num sistema/aplicação/ tecnologia deve ser no máximo cinco. Sempre que suportar, após cinco tentativas falhadas de autenticação a partir do mesmo ponto, o sistema deve bloquear o acesso a esse Utilizador a partir do ponto identificado até que o administrador reinicie a respetiva password (password reset) e o processo de autenticação deve manter-se impedido por um período nunca inferior a 10 minutos;
- Sempre que a segurança de um sistema/ aplicação/ tecnologia tenha sido comprometida ou exista uma suspeita nesse sentido, o responsável pelo mesmo deve:
    - Reiniciar todas as passwords relevantes;
    - Forçar que todas as passwords relacionadas com o mesmo sejam alteradas na próxima vez que cada Utilizador se autentique;
    - Caso não seja possível implementar a recomendação anterior por limitações técnicas, o responsável deve divulgar uma mensagem que notifique todos os Utilizadores e os informe da necessidade de alterar imediatamente as respetivas passwords.
- É proibida a apresentação por uma aplicação/sistema/tecnologia de qualquer password no ecrã ou impressa em papel, devendo sempre ser dissimulada durante a sua inserção;
- Sempre que as aplicações/sistemas/tecnologias o permitam, a password inicial atribuída a um Utilizador deve ser válida apenas durante a primeira autenticação do Utilizador. Durante esse acesso, o Utilizador deve ser forçado a alterar essa primeira password. Este processo também deve ser aplicado sempre que um Utilizador esqueça a sua password e esta tenha de ser reiniciada pela equipa de suporte/manutenção (password resetting);
- Devem ser implementados mecanismos automáticos em sistemas/aplicações/tecnologias que forcem o Utilizador a periodicamente alterar a password de acordo com as seguintes regras:
    - No máximo uma password só poderá ser utilizada durante 90 dias, após o que deve expirar e forçar a sua alteração;
    - Não deve ser possível reutilizar nenhuma das últimas 10 passwords usadas anteriormente;
    - Após a definição da nova password, o Utilizador só a poderá alterar novamente após pelo menos 1 hora;

    a. Os sistemas/aplicações/tecnologias apenas devem permitir passwords que estejam de acordo com as regras

- Os sistemas/aplicações/tecnologias apenas devem permitir passwords que estejam de acordo com as regras de construção definidas no ponto 6.5 ou 6.6.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.17. Authentication information.

6.2.1 Diretrizes especificas de User-Id's e Passwords para Uso Aplicacional

Sempre que um sistema, aplicação ou base de dados target permitir o acesso direto a outros sistemas ou aplicações "clientes", através de um logon sobre um user-id e password, o sistema/aplicação target deve garantir:

- User-id's e passwords distintos, para cada sistema ou aplicação que sejam seus "clientes", independentemente do método de acesso usado;
- As passwords usadas devem seguir as diretrizes de construção de passwords robustas;
- O sistema/aplicação/base de dados target deve recusar o logon se o IP de origem não pertencer a um range reconhecido;
- De forma a prevenir possíveis ataques à segurança da informação, o número de tentativas consecutivas de um sistema/processo para autenticação num outro sistema/aplicação/ tecnologia deve ser no máximo uma;
- Quando um logon falhar quer pela password estar errada quer pelo IP não pertencer ao range esperado, deve falhar sem devolver qualquer feedback à entidade "client";
- Todos os logons quer tenham tido sucesso ou não, devem ser registados em log apropriado, mantido em zona segura.
- De forma a garantir rastreabilidade, os user-Id's e Passwords para uso aplicacional não devem ser utilizados fora do âmbito dos processos e ou procedimentos aplicacionais instituídos (pe.e interfaces, schedulers, pools, etc.) independentemente da função do ambiente. Assim, não podem ser utilizados para ligações diretas de utilizadores individuais, nomeadamente a partir de equipamentos fora do ambiente datacenter.

Caso se verifiquem todos os pontos anteriores e que as aplicações/processos "client" e o sistema/aplicação ou base de dados target residam em zonas seguras dentro de Data Centers do Grupo MEO, as passwords não têm de ser alteradas de forma periódica obrigatória.

Caso contrário, os responsáveis pelo sistema ou processo "client" devem assumir um período de expiração da password (no máximo um ano), e garantir um processo de atualização fiável seguindo as recomendações referidas no ponto 6.2.5 para passwords robustas.

Em qualquer dos casos, sempre que exista uma suspeita fundada de que determinada password foi revelada para além da equipa responsável pela exploração dos sistemas ou tecnologias envolvidas, o administrador responsável de sistema/ aplicação/ tecnologia deve proceder à sua substituição.

A utilização destas contas tem como propósito possibilitar que um Sistemas, Bases de Dados, Plataformas de Serviço, Equipamentos de Rede dos Sistemas e das Tecnologias de Informação e Comunicação, comuniquem umas com as outras, pelo que apenas devem ser utilizadas de forma automática, não sendo permitido a sua utilização por uma pessoa nominal.

Todas as contas aplicacionais devem ter um responsável nominal (não uma entidade, e-mail de suporte ou sigla de departamento) devidamente registado na plataforma centralizada de gestão de identidades (Identity Management do Grupo MEO).

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.18. Access rights, 5.16 Identity management

6.2.2 Diretrizes especificas de User IDs para contas de suporte técnico de SI/TI e de Telco

É permitida a existência de Contas de suporte técnico de SI/TI e de Telco, quer da responsabilidade de colaboradores internos, quer da responsabilidade de colaboradores externos, estes últimos desde que devidamente contratualizadas com as entidades que prestam o suporte aos ativos em causa. Devem ter sempre identificadas um:

- Responsável nominal interno (nome e número de colaborador);
- Responsável nominal da entidade externa.

Estas contas deverão ser acedidas via VPN e ter um perfil estritamente necessário à utilização das plataformas que necessita, no âmbito do que se encontra contratualizado, incluindo também 2FA caso tenham acesso à administração de Sistemas, Bases de Dados, Plataformas de Serviço, Equipamentos de Rede dos Sistemas e das Tecnologias de Informação e Comunicação.

Sempre que se justifique deve ser utilizada uma jump box para acesso a estas aplicações e cujos perfis sejam equivalentes a contas de administração.

Incluem-se nas contas de suporte técnico de SI/TI e de Telco, nomeadamente, as "que vêm de fábrica", as que são essenciais para Operar, Manter e Gerir as mesmas, aceder em caso de incidente grave, e com acesso à administração de Sistemas, Bases de Dados, Plataformas de Serviço, Equipamentos de Rede dos Sistemas e das Tecnologias de Informação e Comunicação.

6.2.3 Diretrizes especificas para Construção de Passwords para Utilizadores Nominais (Internos ou Externos)

Todos os Utilizadores devem estar consciencializados para a importância da escolha de uma password que não seja fraca.

Passwords fracas põem em risco a segurança da informação pelo que são proibidas por esta Política. As passwords nunca devem ser escritas ou registadas em nenhum suporte.

As passwords dos Utilizadores devem ter pelo menos 15 caracteres e garantir a inclusão de 3 dos 4 seguintes conjuntos de caracteres[1]:

- Conter letras minúsculas (a...z)
- Conter letras maiúsculas (A...Z);
- Conter números (0...9)
- Conter carateres especiais: ~!@#$%^&*()+|` -=\{}[]:";'<>?,/

Como boa prática adicionalmente, o Utilizador deve assegurar que:

- Não usa uma palavra em qualquer língua, dialeto ou calão;
- Não utiliza informação pessoal;
- Não contem o respetivo username.
- A password para acesso a ambientes do MEO é completamente diferente de qualquer outra password que utilize para se autenticar em aplicações pessoais (p.e. Linkedin, gmail, Home Banking, etc.)

Em alternativa, podem ser constituídas por frases ou excertos de texto longo conhecidos pelo Utilizador, adicionando caracteres especiais em substituição de algumas letras (exemplo: S por $, B por 3, A por 4, O por 0, etc...), sem caracter de «espaço» e com um mínimo de 40 caracteres.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 5.16 Identity management.

6.2.4 Diretrizes especificas para Construção de Passwords Robustas para Utilizadores com Privilégios de Administração

As passwords de Utilizadores nominais com privilégios de administração, devem ser robustas de acordo com as características acima e adicionalmente terem pelo menos 22 caracteres.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.16 Identity management

6.2.5 Diretrizes especificas para Construção de Passwords Robustas para Utilizadores/ "User-Id's e Passwords para Uso Aplicacional"

As passwords de Utilizadores/ User-Id's e Passwords para Uso Aplicacional com privilégios de administração, e para integração aplicacional, devem ser robustas de acordo com as características acima e adicionalmente terem pelo menos 22 caracteres.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.16 Identity management

6.3 Responsabilidades Específicas dos Utilizadores

6.3.1 Segurança das Estações de Trabalho (ET) (VDi's, Desktops e Notebooks)

É proibido aos Utilizadores:

a. Efetuar ações que possam danificar, interromper ou gerar erros nos sistemas informáticos;
b. Efetuar uploads, downloads ou transmissão não autorizada de qualquer programa ou ficheiro sobre o qual incidam direitos de autor, direitos conexos ou outros direitos de propriedade intelectual, nomeadamente ficheiros de música, vídeos, etc., para fins não profissionais;
c. Proceder à instalação de cookies.

Todas as ET, independentemente de serem VDi's, Desktops ou Notebooks, devem ser instaladas pela estrutura do MEO responsável pela gestão de desktops, e devem garantir suporte ativo ao conjunto de mecanismos de proteção estipulados pelas regras de segurança em vigor no MEO: Anti-Spam, Anti-Malware, Personal Firewall, Screen-saver ativo com password, XDR/EDR, DLP, etc. Estes mecanismos devem estar sempre ativos e devem ser automaticamente atualizados. Os Utilizadores não podem alterar estas configurações na ET de forma a garantir a segurança da informação no uso da mesma.

Exceções a esta regra devem ser autorizadas pela entidade responsável pelas ET.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.7 Protection against malware, 5.17 Authentication information, 8.12 Data leakage prevention.

6.3.2 Segurança das Estações de Desenvolvimento (TD) (Desktop s ou Notebooks)

Todas as TD devem ser instaladas pela estrutura do Grupo MEO responsável pela gestão de desktops, e devem garantir suporte ativo ao conjunto de mecanismos de proteção estipulados pelas regras de segurança em vigor: Anti-Spam, Anti-malware, Personal Firewall, Screen-saver ativo com password XDR/ EDR, DLP, etc. Estes mecanismos devem estar sempre ativos e ser atualizados automaticamente. A alteração destas configurações, bem como a instalação/ desinstalação de software, é da responsabilidade do Utilizador a quem a estação de desenvolvimento foi atribuída.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.7 Protection against malware, 5.17 Authentication information, 8.12 Data leakage prevention

6.3.3 Segurança das Estações de Trabalho (ET) com acesso a contas privilegiadas de Administração

Nas ET com acesso a contas privilegiadas de Administração, por princípio, os dados armazenados no seu disco devem estar sujeitos a processo de encriptação, devendo este princípio ser aplicado a quaisquer outros Mobile Device (p.e. Tablets, etc.) que tenham acesso a dados classificados do Grupo MEO.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.7 Protection against malware, 5.17 Authentication information

6.3.4 Segurança dos Devices não geridos pelas áreas técnicas do Grupo MEO

Todo e qualquer device que se tente ligar à rede do Grupo MEO, quer por rede fixa, quer por rede wireless, deve cumprir os requisitos de segurança definidos para as ET geridas pelo Grupo MEO. Caso não cumpra esses requisitos, deverá ficar limitado à Internet pública e qualquer acesso a sistemas, tecnologias e aplicações do Grupo MEO, terá de ser efetuado com recurso a uma VPN (Virtual Private Network) oficial do Grupo MEO classificada para lidar com devices não geridos ou via interface tipo Citrix.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.7 Protection against malware, 5.17 Authentication information, 8.12 Data leakage prevention

6.3.5 Lock e Logout das Estações de trabalho (ET)

Utilizadores que deixem o seu posto de trabalho sem supervisão devem previamente garantir que efetuam o Lock ou Logout do seu computador.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.17 Authentication information

6.3.6 Proteção das Passwords

Todas as passwords devem ser tratadas como informação classificada da organização. As passwords nunca devem ser partilhadas com ninguém.

Os Utilizadores não devem utilizar a mesma password para acessos no Grupo MEO e para acessos externos à mesma, e não devem:

- Revelar a sua password por telefone a ninguém;
- Revelar a sua password em nenhuma mensagem de e-mail;
- Revelar a sua password à sua chefia;
- Falar de uma password na presença de outras pessoas;
- Revelar pistas sobre a sua password (p.e., “o meu nome de família”);
- Revelar a sua password em inquéritos ou outros meios;
- Revelar a sua password a colegas quando vão de férias;
- Partilhar a sua password com membros da família;
    - Utilizar a funcionalidade “Remember Password” disponível em algumas aplicações (p.e., OutLook, Netscape Messenger);

- Escrever a password e guardá-la no escritório ou em qualquer dispositivo, incluindo no computador ou dispositivo móvel de forma não cifrada.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.17 Authentication information

6.3.7 Partilha de Informação

A partilha de discos com privilégios de leitura/escrita é proibida. Para a partilha de informação devem ser utilizados os sistemas existentes na organização (p.e., Shares, Intranets, Sharepoint, etc.) para os quais se encontram definidas e implementadas as necessárias políticas de acesso.

Se a partilha de informação tiver que ser efetuada por dispositivo de armazenamento externo (por impossibilidade técnica) o dispositivo deve ser cifrado ou protegido por password.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.2 Privileged access rights, 5.17 Authentication information, 8.12 Data leakage prevention

6.3.8 Comunicação de Situações Anómalas

Sempre que um Utilizador suspeite do uso indevido da sua conta de acesso a um sistema/ aplicação/ tecnologia, ou que a sua password tenha sido revelada, deve informar imediatamente o SOC de acordo com o descrito no capítulo 9 desta Política – Comunicação de Incidentes de Segurança.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 6.8 Information security event reporting

6.3.9 Destruição e/ ou Alteração não Autorizada de “Logs” Aplicacionais ou de Sistema

Os Utilizadores não podem destruir, alterar ou comprometer quaisquer logs aplicacionais ou de sistema. O não cumprimento desta regra constitui uma violação grave a esta Política.

Os LOGs devem ser armazenados em ambiente seguro e segregado dos ambientes onde esses eventos foram gerados e digitalmente assinados. É recomendável a segregação das equipas que gerem os ambientes onde esses eventos têm origem e as equipas que gerem o armazenamento dos LOGs. Os LOGs devem registar os eventos relevantes segundo o princípio do CRUD (Create, Read, Update, Delete), bem como permitir responder às questões: Quem fez?; Quando fez?; Como Fez?; De onde Fez?; O que Fez?; Porque Fez?.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.17 Authentication information

6.3.10 Realização de Testes Não Autorizados de Segurança

Os programas de testes e demonstração que não pertençam ao Grupo MEO só podem ser utilizados após exame e autorização prévia por parte da entidade responsável pela Segurança da Informação.

Os Utilizadores não podem executar operações informáticas que constituam uma violação de quaisquer disposições legais aplicáveis. Os Utilizadores não podem testar ou comprometer as medidas de segurança associadas aos sistemas.

Incidentes envolvendo captura e análise de tráfego (network tapping ou sniffing), tentativa de acesso não autorizado a sistemas, aplicações ou plataformas de comunicações, password cracking, decifração de ficheiros de terceiros, ou outras atividades similares geralmente classificadas como hacking, que podem comprometer a segurança dos sistemas e tecnologias de informação e comunicação, são consideradas violações graves desta Política.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 8.7 Protection against malware, 5.17 Authentication information.

6.3.11 Máquinas de Salto ou JumpBoxes

No caso de impossibilidade em identificar todos os IP autorizados (p.e., IP's atribuídos via DHCP) os acessos devem ser efetuados via entreposto de administração (conhecido como Máquina de Salto ou JumpBox) reconhecido pela entidade responsável pela operacionalização e gestão dos serviços de TI's.

Apenas devem ter privilégios de administração (Sistemas, Base de Dados, Aplicações, etc.) técnicos autorizados, nominalmente identificados e sujeitos à assinatura de uma Declaração de Confidencialidade ou a regras de confidencialidade no âmbito da relação laboral com as empresas do Grupo MEO.

Em todos os sistemas da família UNIX deve ser proibido o login direto a root. Os administradores de sistemas ou responsáveis pela operação devem fazer primeiro login em conta própria nominal, que tenha apenas os privilégios estritamente necessários para a sua função, e sempre que necessário, e só nessas circunstâncias, fazer SUDO a root a partir da sua conta nominal.

Acessos SNMP são estritamente proibidos a entidades não autorizadas. Acessos SNMP não seguros são proibidos.

Todos os sistemas e tecnologias novas devem suportar SSH para acessos interativos ao sistema, mesmo dentro de um perímetro seguro. Devem ser evitados acessos utilizando protocolos não seguros.

Na realização de RFP's (Request For Proposal) deve ser tido em conta que:

- Todos os novos sistemas e tecnologias de informação e comunicação devem suportar Protocolos Seguros para a sua gestão remota (p.e., SSH);
- Todos os novos sistemas e tecnologias de informação e comunicação devem suportar a última versão do SNMP.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.20 Networks security, 8.24 Use of cryptography.

6.3.12 Remote Shells , SNMP e Administração de Sistemas e Tecnologias de Informação e Comunicação

Nas situações em que é inviável a utilização de tecnologias do tipo JumpBox para acesso a sistemas e tecnologias legadas que, por razões técnicas históricas, só tenham Telnet ou outro protocolo idêntico de remote Shell, SNMP não seguro, os acessos devem ser apenas permitidos dentro de um perímetro seguro e a partir dos IP's específicos das consolas autorizadas, devendo o acesso estar bloqueado para qualquer outro IP.

6.3.13 Outras Disposições

Como parte desta Política, o Grupo MEO instala em todos os devices geridos dos seus colaboradores (p.e., ET) sistemas de segurança como anti-vírus/anti-malware. O facto destes sistemas de segurança examinarem os CDs/ DVDs ou dispositivos de armazenamento de informação do Utilizador, o seu funcionamento não

implica a autorização deste.

Os recursos informáticos e de comunicação são disponibilizados pelo Grupo MEO como instrumentos de trabalho auxiliares ao desempenho da atividade contratada, constituindo a possibilidade da sua utilização para fins privados uma liberalidade da empresa. O Grupo MEO reserva o direito, sem prejuízo da manutenção da vigência da presente Política, de revogar em qualquer altura, e sem aviso prévio, a utilização desses recursos para fins profissionais e/ou pessoais, com a inerente obrigação do Utilizador os entregar imediatamente.

6.3.14 Obrigações no Momento de Cessação de Vínculo Laboral ou Contratual

Em caso de cessação do contrato de trabalho ou mudança de funções, o Utilizador é obrigado a:

a. Entregar ao seu superior hierárquico os equipamentos, software e demais ferramentas de trabalho e informação elaborada e/ou em seu poder, não podendo conservar ou utilizar a referida informação para qualquer efeito, sem autorização prévia e escrita do Grupo MEO;
a. Eliminar toda a informação de natureza pessoal que tenha armazenado ou que se encontre disponível nos sistemas da empresa e nos recursos eletrónicos disponibilizados pela mesma;
b. Entregar os e-mails de caráter profissional ao seu superior hierárquico, em formato digital.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection Information Security Management Systems – Requirements, controls, 5.17 Authentication information

6.4 Controlo de Acessos à Rede

6.4.1 Acesso à Internet

Acesso de utilizadores à internet deve ser feito através do Proxy do MEO e aceite os grupos e categorias já definidos. Exceções devem ser avaliadas de acordo com o Ponto 8 (Exceções e Pareceres à Política de Segurança da Informação) e aprovado pela Direção de Cybersecurity.

6.4.2 Utilização simultânea de várias redes

Enquanto um Desktop ou notebook estiver ligado a uma das redes internas do Grupo MEO não pode estar ligado a qualquer outra rede.

A utilização de kits ADSL, Modems ou dispositivos móveis de acesso à internet para ligação, de Desktops ou notebooks, simultaneamente à Internet e a qualquer das redes internas do Grupo MEO (incluindo redes de gestão) é proibida.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 5.15 Access control.

6.4.3 Utilização de Redes Wireless

A área responsável pela segurança operacional das redes internas deve assegurar que apenas os acessos wireless que garantam a segurança da informação dos Utilizadores são autorizados a operar nas instalações das empresas, tendo de lhes ser submetido previamente o pedido de autorização de ligação dos dispositivos.

Pontos de Acesso, dentro de instalações do Grupo MEO e com ET ou TD do Grupo MEO, a redes wireless não autorizadas são consideradas violações graves a esta Política.

É considerada violação grave, toda e qualquer instalação de equipamentos wireless (p.e., routers com interface WiFi) não autorizados e que disponibilizem a outros equipamentos um acesso direto à rede interna do Grupo MEO.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.15 Access control, 8.20 Networks security.

6.4.4 Túneis para o Exterior

A abertura de túneis que permitam a comunicação de dados a partir da rede interna do Grupo MEO para o exterior, sem ser devidamente analisada, documentada e autorizada pelas chefias correspondentes e pela entidade responsável pela Política de Segurança da Informação, é expressamente proibida.

Não é permitida a utilização de mecanismos de anonimização de navegação na internet, como por exemplo a utilização de TOR Networks, por contas de utilizadores do Grupo MEO. Uma vez que este tipo de mecanismos inviabilizam a rastreabilidade de quem utiliza os recursos do Grupo MEO.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 5.15 Access control, 8.20 Networks security.

6.4.5 Acessos Remotos via VPN

Os acessos remotos para o interior da empresa devem recorrer sempre, a VPN's oficiais geridas pela entidade responsável pela Infraestrutura.

Os pedidos de acesso a partir do exterior devem ser devidamente analisados, documentados e autorizados pelas chefias. Esses pedidos são suportados num procedimento que garante a rastreabilidade dos acessos atribuídos e a preservação destes registos pelo período de 2 anos.

No acesso remoto a equipamento deve utilizar-se apenas Protocolos Seguros, sempre que os sistemas o permitam.

Não é permitida a utilização de mecanismos de anonimização para acessos remotos ao Grupo MEO, como por exemplo via TOR Networks. Uma vez que este tipo de mecanismos inviabilizam a rastreabilidade de quem utiliza os recursos do Grupo MEO.

Todos os Utilizadores com privilégios de administração e perfis de acesso não restrito na VPN Corporativa deverão ter de usar 2FA na autenticação logo na VPN.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.15 Access control, 8.20 Networks security, 6.7 Remote working, 8.12 Data leakage prevention.

6.4.6 Acessos Remotos via Citrix

Os acessos remotos, a partir do exterior, a aplicações corporativas via plataforma Citrix, devem ser devidamente analisados, documentados e autorizados pelas chefias. Esses pedidos são suportados num procedimento que garante a rastreabilidade dos acessos atribuídos e a preservação destes registos pelo período de 2 anos.

Não é permitida a utilização de mecanismos de anonimização para acessos remotos ao Grupo MEO, como por exemplo via TOR Networks. Uma vez que este tipo de mecanismos inviabilizam a rastreabilidade de quem utiliza os recursos do Grupo MEO.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 5.15 Access control, 8.20 Networks security, 6.7 Remote working, 8.12 Data leakage prevention.

6.4.7 Acessos a Extranet(s)

Todos os pedidos de novas ligações a uma extranet devem ser formalizados por escrito pela entidade requisitante junto da equipa responsável pela extranet, incluindo uma justificação do requisito de negócio subjacente. Estes acessos devem ser revistos e autorizados, de modo a assegurar que estão de acordo com os requisitos de negócio e políticas definidas e que o princípio de "acesso apenas ao que é necessário" é cumprido. As alterações a um acesso já existente são requeridas seguindo o mesmo processo de um novo pedido.

A disponibilização de novas conexões entre terceiras partes e o Grupo MEO tem de ser formalizada através de contrato, o qual deve estar em conformidade com os termos da presente Política.

Quando um acesso extranet já não é necessário, a entidade requerente deve notificar a equipa responsável, para desativar esse acesso. Esta ação poderá corresponder a uma modificação das permissões existentes ou à desativação total dessa conexão.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 5.15 Access control, 8.20 Networks security.

6.5 Controlo de Acessos a Sistemas Operativos

6.5.1 Diretrizes de Configuração de Estações de Trabalho (ET e TD)

As ET de todos os colaboradores devem ter um Antivírus, Anti-Spyware e Personal Firewall ativos e com atualizações automáticas. O Utilizador da TD deve ser impedido de alterar a configuração destes programas. No caso de Estações de Trabalho Virtuais (VDi's) os mecanismos de proteção equivalentes devem ser implementados ao nível da plataforma de virtualização e não necessariamente ao nível de cada Desktop Virtual.

O screen saver deve estar configurado para, após cinco minutos de inatividade no posto de trabalho, o mesmo ser ativado protegendo o acesso por password.

Na altura da autenticação dos Utilizadores que pretendem utilizar um posto de trabalho, os servidores de domínio devem validar e forçar a configuração de segurança acima referida. Caso o posto de trabalho não cumpra com algum dos critérios, a sua entrada na rede deve ser recusada.

Em circunstância alguma devem ser permitidos Desktops ou Notebooks ligados à rede interna sem que estes tenham Utilizadores autorizados.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 8.3 Information access restriction.

6.5.2 Diretrizes de Configuração de Estações de Trabalho de Risco

Qualquer ET deve ser instalada de acordo com as regras de segurança em vigor no Grupo MEO, incluindo ativações de Anti-Spam, Anti-Malware, Personal Firewall, Screen-saver ativo com password, XDR/EDR, DLP, etc., bem como atualizações automáticas, estando os Utilizadores proibidos de alterar as respetivas configurações, salvo com prévia autorização da entidade responsável pela aplicação em causa.

Entende-se como ET de risco, as que se encontram mais expostas a ameaças e como tal apresentando maior risco de utilização por Utilizadores não autorizados, como por exemplo as lojas e call centers do Grupo MEO, tendo estas acesso e privilégios de utilização mais restritos. Qualquer Utilizador que se autentique numa destas ET terá apenas acesso à funcionalidade e aplicações definidas para o perfil deste posto de trabalho.

O screen saver deve estar configurado para ativar após dois minutos de inatividade no posto de trabalho, protegendo o acesso por password, de forma a prevenir acessos não autorizados por ausência do Utilizador.

Estas Estações de Trabalho de risco não devem ter disponíveis as drives para meios amovíveis, diminuindo assim o risco da existência de cópias não autorizadas da informação.

No caso de ET virtuais (VDi's) sem qualquer possibilidade de ler ou escrever dados e programas a partir de drives USB, CD/DVD ou outros, podem ser implementados mecanismos de proteção equivalentes ao nível da plataforma de virtualização e não ao nível de cada "Desktop Virtual".

Sempre que estas ET de risco sejam suportadas em Laptops/Notebooks, por princípio, os dados armazenados no seu disco devem estar sujeitos a processo de encriptação, devendo este princípio ser aplicado a quaisquer outros Mobile Device (p.e. Tablets, etc.) que tenham acesso a dados classificados do Grupo MEO.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 5.15 Access control, 8.3 Information access restriction, 8.12 Data leakage prevention.

6.5.3 Acessos a Servidores e outras Tecnologias de Informação

Todos os servidores, sistemas de storage e backup e outras tecnologias de informação críticas para o Grupo MEO, devem estar sob a responsabilidade de um grupo operacional que assegure a sua administração, operacionalidade e segurança. Os servidores devem estar sempre localizados num ambiente em que exista um rigoroso controlo de acessos físicos, bem como condições ambientais adequadas para a manutenção do equipamento/ sistemas, bem como a garantia da disponibilidade em termos de fontes energéticas redundantes, de acordo com o risco do ativo em causa.

6.5.4 Acessos a Elementos de Rede e Segurança de Redes

Todos os routers, switches, firewalls, IDS's, IPS's e outros elementos de redes do Grupo MEO devem estar sob a responsabilidade de grupos operacionais que assegurem a sua administração e segurança. Estes elementos de rede devem estar sempre localizados em ambientes em que exista um controlo de acessos físicos, e condições ambientais adequadas para a sua operação e manutenção, bem como a garantia da disponibilidade em termos de fontes energéticas redundantes, de acordo com o risco do ativo em causa.

6.5.5 Diretrizes de Configurações

A configuração dos sistemas operativos deve ser sempre efetuada tendo em consideração as normas de segurança emitidas pelos respetivos fornecedores e elaboradas pelas áreas operacionais. O acesso a serviços deve ser protegido por mecanismos de controlo de acessos, por exemplo Host Firewalls.

Devem ser instalados os patches de segurança de acordo com as políticas de distribuição em vigor, exceto quando se verificar que a sua aplicação imediata interfere com um requisito de negócio. As relações de confiança entre sistemas são um risco de segurança, devendo ser evitado o seu uso. Esta solução só pode ser utilizada se não existir nenhuma opção de comunicação alternativa.

Os privilégios de acesso devem ser definidos tendo por base o princípio que cada Utilizador só pode executar as ações estritamente necessárias na sua função.

Sempre que exista disponível um canal de comunicação seguro (se for tecnicamente exequível), os acessos privilegiados só devem ser efetuados sobre estes canais (p.e., conexões cifradas utilizando: HTTPS, SSH, SSL/TLS, SFTP, SCP, IPSec, etc.).

É proibido aos Administradores de servidores e ativos de rede:

a. Efetuar ações que possam danificar, interromper ou gerar erros nos sistemas informáticos;

b. Efetuar uploads, downloads ou transmissão não autorizada de qualquer programa ou ficheiro sobre o qual incidam direitos de autor, direitos conexos ou outros direitos de propriedade intelectual, nomeadamente ficheiros de música, vídeos, etc., para fins não profissionais.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 5.15 Access control, 8.3 Information access restriction, 7.8 Equipment siting and protection.

6.5.6 Passwords de Bases de Dados

As aplicações disponíveis na rede do Grupo MEO que necessitem de aceder a um ou mais servidores de Base de Dados têm de se autenticar através da apresentação das credenciais necessárias. Estas credenciais não devem residir no corpo do código da aplicação em texto, nem ser armazenadas numa localização acessível através de um web server ou da utilização de protocolos inseguros.

6.5.7 Armazenamento de User Names e Passwords de acesso a Bases de Dados

- Os User Names e Passwords de acesso a Bases de Dados podem ser guardados em zona segura num ficheiro separado do código da aplicação.
- Se estiverem guardados num ficheiro, os User Names e Passwords de acesso a Bases de Dados devem ser lidos no momento anterior à sua utilização. Imediatamente a seguir à autenticação na Base de Dados, a memória contendo o User Name e Password deve ser limpa ou libertada.
- As credenciais de Base de Dados podem residir no servidor. Neste caso, um número de hash que identifique as credenciais poderá estar incluído no código da aplicação.
- As credenciais de Base de Dados podem residir num servidor de autenticação, tal como um servidor LDAP utilizado para autenticação de Utilizadores. A autenticação da aplicação na Base de Dados pode ocorrer como parte do processo de autenticação de Utilizador no servidor de autenticação. Neste caso, não existe necessidade de utilização de credenciais ao nível da programação da aplicação.
- As credenciais de Base de Dados não podem residir na árvore de documentos de um web server.
- A autenticação de Utilizadores de Base de Dados Oracle nunca deve usar o mecanismo Oracle que delega essa tarefa no sistema operativo do cliente, também conhecido por autenticação OPS$.
- Para linguagens executáveis a partir do código, as respetivas credenciais não devem residir no mesmo diretório onde se encontra o código-fonte.
- As passwords utilizadas para acesso a Base de Dados devem estar de acordo com as diretrizes de criação de Passwords Robustas.

6.5.8 Acesso a User Names e Passwords de Bases de Dados

Cada aplicação que implemente uma função de negócio deve ter credenciais únicas de Bases de Dados.

As equipas responsáveis pelas Bases de Dados devem ter um processo definido que garanta que as passwords de Bases de Dados são controladas e incluir também um método para restringir o seu conhecimento apenas a quem necessita. A partilha de credenciais por diversas aplicações não é permitida.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 8.3 Information access restriction.

6.5.9 Passwords de Acesso a Aplicações

Mesmo nas aplicações residentes em zonas seguras dentro de um Data Center, não deve haver passwords diretamente escritas no código aplicacional, em scripts nem em ferramentas e/ou mecanismos de automação. Se não houver alternativa prática, face à base tecnológica em uso (p.e. tecnologias obsoletas), deve garantir-se que as passwords residem em ficheiro próprio devidamente protegido e encriptado e só acessível à aplicação ou script que dela precisa.

Sempre que as aplicações armazenem os identificadores dos seus Utilizadores e as respetivas passwords, dentro de uma tabela numa base de dados, devem fazê-lo de forma cifrada, para ambas as colunas (login e password). A chave de cifra não deve ser armazenada dentro da base de dados, recomendando-se a utilização de um ficheiro de configuração da aplicação com acesso protegido.

Quando a componente "client" de uma aplicação, a funcionar num desktop/notebook, precisar de aceder diretamente a outra aplicação secundária, deve obrigar o Utilizador a fazê-lo explicitamente ou recorrer ao processo de Single-Sign-On do Grupo MEO.

As aplicações novas que lidem com informação classificada devem garantir autenticação via rede através de Protocolos Seguros com base criptográfica (p.e., HTTPS, SSH, SSL/TLS, ou IPSec).

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 8.3 Information access restriction.

6.5.10 Monitorização de Acessos

Os sistemas operativos, bases de dados e aplicações devem funcionar com o sistema de monitorização de acessos ativo. No nível mínimo de funcionamento, este sistema deve registar entradas e saídas assim como acessos a dados classificados (Confidencial, Reservado, dados de cliente, dados de negócio ou outro tipo de dados protegidos por legislação).

Os sistemas e tecnologias mais críticos, todas as DMZ's, todos os dispositivos de segurança, e todos os sistemas e elementos de rede mais relevantes, devem estar sob monitorização no SOC do Grupo MEO.

Devem ser estabelecidos processos de monitoria que permitam:

Monitoring processes must be established that allow:

- Detect Detetar entradas ou tentativas de entradas ilegítimas nos sistemas;
- Detetar falhas de autenticação;
- Detetar práticas que coloquem em risco a salvaguarda do controlo de acessos;
- Detetar tentativas para aumentar os privilégios atribuídos;
- Garantir a existência de provas suficientes, quando algum incidente ocorrer;
- Definir modelos de comportamento anormais, que permitam detetar cenários anómalos.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 8.15 Logging.

6.6 Standards para Desenvolvimento de Aplicações ou aquisição de aplicações a terceiros

As equipas de desenvolvimento e entidades internas responsáveis pela aquisição e implementação de aplicações adquiridas a terceiros, devem garantir que as soluções por elas desenvolvidas, adquiridas/ implementadas contêm as seguintes precauções de segurança:

1. As aplicações devem suportar a autenticação de Utilizadores individuais (nominalmente identificados) e não de grupos;
2. As aplicações devem ter capacidade para autenticar e autorizar todos os utilizadores e dispositivos, incluindo o controlo do acesso a sistemas e aplicações, nomeadamente Front-ends, devendo ser utilizado sempre que possível e para novos sistemas:
   a. o uso de TLS (Transport Layer Security), na sua versão mais recente;
   b. o uso de password, preferencialmente em combinação:
      - Password + SMS Token
      - Password + Smartcard
      - Password + Biometria
      - Password + Padrão gráfico
      - Password + Cartão de coordenadas
      - Password + Código aleatório temporário (menos de 5 minutos de validade) enviado na forma de QR -Code.

   Estas diretrizes são obrigatórias a todas as aplicações que estejam expostas à internet.
3. Devem providenciar um nível de perfis que permita suportar as diferentes funções de negócio dos Utilizadores, assegurando a segregação de funções e garantindo assim o nível de autorização associado.
4. Devem providenciar algum tipo de gestão de perfis, para que um Utilizador possa assumir as funções de outro sem que tenha de saber a password do colega;
5. O processo de desenvolvimento deve assegurar, que a entidade responsável pelo desenvolvimento executa testes de segurança, para além dos testes funcionais. Adicionalmente, as aplicações expostas à Internet ou às diferentes extranets que lidem com informação classificada devem ser periodicamente testadas contra vulnerabilidades de segurança (p.e., buffer overflows, sql injection, etc.) por parte de uma entidade independente do desenvolvimento;
6. Os eventos de sistema e os de Event log de sistemas, Bases de dados, Aplicações, Ativos de rede, etc., devem ser armazenados em LOGs, digitalmente assinados, em ambiente seguro e segregado dos ambientes onde esses eventos foram gerados. É recomendável a segregação das equipas que gerem os ambientes onde esses eventos têm origem e as equipas que gerem o armazenamento dos LOGs. Os LOGs devem registar os eventos relevantes segundo o princípio do CRUD (Create, Read, Update, Delete), bem como permitir responder às questões: Quem fez?; Quando fez?; Como Fez?; De onde Fez?; O que Fez?; Porque Fez?. Este princípio deve ser utilizado, por omissão, em qualquer tipo de LOG.
7. As aplicações que lidem com informação classificada devem garantir um audit trail que cumpra o princípio do CRUD, em particular às alterações a essa informação classificada indicando, no mínimo:
   - Operação realizada (só obrigatória para informação classificada acima de Confidencial);
   - Alteração feita (valor antigo, valor novo);
   - Estado da operação (p.e., sucesso ou insucesso);
   - Timestamp da operação;
   - Quem realizou a operação (user-id);
   - IP Origem/ Port.
8. Esta informação deve estar disponível por um período mínimo a definir para cada uma das aplicações, devendo também ser definido, em função da finalidade e necessidade da recolha dessa informação, o período máximo de conservação da mesma, de modo a garantir o cumprimento das leis de proteção de dados, nomeadamente no que toca à eliminação de informação contendo dados pessoais. Os prazos de conservação de logs também podem variar em função do contratualizado com

cada cliente ou para cada serviço;

9. Deve suportar TACACS+, RADIUS, LDAP, Single Sign On ou similares sempre que possível;
10. Deve garantir que em ambiente não produtivo não são utilizados dados pessoais provenientes de ambiente produtivo, e caso tal seja necessário, os mesmos devem estar sujeitos a um processo de mascaramento, não permitindo a identificação unívoca do titular dos dados pessoais de forma direta ou indireta, equivalente a anonimização.
11. Deve ser garantido a separação entre ambientes, nomeadamente, Desenvolvimento, Testes e Produção e que o código-fonte fonte não esteja disponível em ambientes Produtivos.
12. Os ambientes não produtivos devem ter os patches e antivírus atualizados a exemplo do que acontece em ambientes produtivos.

Os acessos a ambientes não produtivos, devem observar os requisitos da presente Política em termos de acessos, nomeadamente na componente de contas nominais para o acesso a Sistemas, Bases de Dados, Plataformas de Serviço, Equipamentos de Rede dos Sistemas e das Tecnologias de Informação e Comunicação.

No caso dos ambientes de Laboratório e Desenvolvimento dos Operational Support Systems (OSS) das áreas de telecomunicações devem ser garantidos os seguintes requisitos:

- Separação adequada, idealmente a nível de HW, entre ambientes de desenvolvimento/laboratório e de produção;
- Separação adequada entre a rede do laboratório e a rede corporative;
- Isolamento adequado (ex: através de VDI) entre os dispositivos de acesso aos ambientes de laboratório, aos ambientes de produção e à rede corporativa/redes externas.

Caso as condições acima sejam satisfeitas, os fornecedores/subcontratados para desenvolvimento/teste podem utilizar aplicações de partilha de desktop para debugging em ambiente de laboratório e desenvolvimento.

As diretrizes referidas anteriormente deverão ser tidas em consideração em todos os projetos de renovação tecnológica e sempre que possível atualizadas.

As Direções responsáveis pela concretização de novos projetos, que venham a resultar em novas aplicações ou novos Sistemas e Tecnologias de Informação e Comunicação, são responsáveis por garantirem o cumprimento desta Política.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.3 Information access restriction, 8.26 Application security requirements, 8.10 Information deletion.

7 Disposições Adicionais na Gestão e Administração de Sistemas, Bases de Dados e Aplicações

7.1 Garantia de Zonas Seguras (Perímetros Seguros)

Todos os sistemas e aplicações relevantes devem estar, sempre que possível, em perímetros seguros, tanto ao nível físico como lógico. Apenas os front-ends aplicacionais devem ficar expostos numa DMZ.

Ao nível da segurança física, para um perímetro ser considerado seguro, terá de estar totalmente protegido dentro de um Data Center do Grupo MEO e o acesso físico ao mesmo terá de implicar a identificação, autorização, controlo e acompanhamento de quem quer que pretenda o acesso.

Os locais onde estão localizadas as infraestruturas têm de possuir mecanismos que permitam gerar eventos relativos aos acessos físicos realizados ou tentados.

Ao nível da segurança lógica, para um perímetro ser considerado seguro, terá de garantir que todos os acessos por rede a qualquer dos sistemas ou tecnologias dentro ou nesse perímetro sejam previamente conhecidos, monitorizados e controlados por sistemas de segurança operacional (Firewalls e IDS's/IPS's) e devidamente integrados no SOC do Grupo MEO. Adicionalmente, um perímetro só será considerado seguro se todos os sistemas e elementos de rede nele contido estiverem seguros de acordo com as melhores práticas de segurança de informação e não exista qualquer relação de confiança entre um sistema dentro do perímetro seguro e um outro sistema fora desse perímetro. Um perímetro seguro exige que a sua administração, quando remota, recorra a Protocolos Seguros e a consolas seguras.

A entidade responsável por esta Política de Segurança da Informação deve, sempre que considere necessário, efetuar peritagens à segurança lógica e física dos perímetros seguros do Grupo MEO.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 8.3 Information access restriction, 8.22 Segregation of networks.

7.2 Hardening de Sistemas, Bases de Dados, Aplicações e Elementos de Rede

Deve ser garantido que em todos os sistemas, bases de dados, aplicações e elementos de rede se elimine o maior número de possíveis riscos de segurança, desabilitando contas, serviços, interfaces (incluindo portas IP) desnecessárias à sua função final.

Em particular, os front-ends aplicacionais Web expostos na internet/extranet devem ser sujeitos a security hardening, de acordo com normativo interno que segue as melhores práticas internacionais, p.e., NIST (www.nist.org), SANS (www.sans.org) ou CIS (https://www.cisecurity.org/). Os sistemas que deixem de ter funções operacionais, porque foram entretanto substituídos por sistemas mais atuais, ou por qualquer outra razão, não devem permanecer acessíveis nas redes internas do Grupo MEO. Enquanto não forem definitivamente desligados ou reaproveitados para outras funções, devem permanecer sob controlo da segurança operacional do respetivo Data Center ou salas técnicas do tipo ANG (Áreas de Nova Geração).

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 8.7 Protection against malware.

7.3 Acessos a Execução de Comandos

Apenas devem ter privilégios de administração (Sistemas, Base de Dados, Aplicações, Plataformas de Serviço, elementos de Rede, etc.) os técnicos nominalmente identificados e sujeitos à assinatura de uma Declaração de Confidencialidade ou a regras de confidencialidade no âmbito da relação laboral com empresas do Grupo MEO.

Para sistemas da família UNIX/Linux não devem ser efetuados acessos root remotos diretamente.

Nos sistemas da família Windows, o acesso direto com privilégio de Administrador, deve ser garantido através de PowerShell atualizado e configurado com as melhores práticas, nomeadamente cumprindo o princípio do privilégio mínimo necessário à ação a desempenhar, e sempre que possível via JumpBoxes.

Deve ser sempre feito o acesso como Utilizador nominal e posteriormente elevar privilégios para root, garantindo que existem audit logs do processo.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 8.3 Information access restriction.

7.4 Aplicação de Patches

Deve ser garantido pelos responsáveis de cada sistema, que todos os patches lançados pelo fabricante, especialmente os patches relativos à segurança, estejam devidamente instalados no sistema, com a exceção de causar impacto no bom funcionamento dos sistemas.

Estas atualizações devem ser formalmente planeadas, devendo ser identificados os riscos associados e definidos os planos de testes e os procedimentos de fall-back, de acordo com procedimento interno da equipa responsável pelo IT.

Como Patches estão incluídos todos os aplicáveis a Endpoints, Servidores, Bases de Dados, Plataformas de Serviço e Networking, nas componentes de Sistema Operativo e Aplicacionais, devendo o detalhe de aplicabilidade dos mesmos ser definido em normas específicas de quem garante a Operação, Manutenção e Gestão, mediante parecer da Direção de Cybersecurity.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 8.7 Protection against malware, 8.32 Change management, 8.8 Management of technical vulnerabilities.

7.5 Descontinuação de Sistemas e Elementos de Rede

A descontinuação de Sistemas e Elementos de Rede encontra-se definida em procedimentos específicos do Grupo MEO.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 5.9 Inventory of information and other assisted assets, 5.11 Return of assets, 5.23 Information security for use of cloud services, 8.20 Networks security, 8.21 Security of network services.

8 Exceções e Pareceres à Política de Segurança da Informação

Para qualquer das disposições acima definidas pode ser usado o procedimento de gestão de exceções para justificar atividades que não cumpram o estabelecido nesta Política.

Podem existir casos de exceções, que por requisitos de negócio ou porque existem controlos compensatórios estão previamente aprovadas. Estas situações estão detalhadas no Procedimento de Gestão de Exceções. Relativamente a qualquer situação relacionada com Política de Segurança da Informação que não esteja coberta pela mesma, pode solicitar-se parecer vinculativo à Direção de Cybersecurity.

Sempre que se justifique podem ser definidas políticas específicas, as quais não podem derrogar nenhuma das diretrizes definidas na presente Política, as quais se encontram documentadas em repositório da organização. A aprovação das mesmas é efetuada pela Direção de Cybersecurity.

8.1 Sistemas e Tecnologias novos ou já existentes e não incluídos no Manual de Controlo Interno

Para os novos Sistemas e Tecnologias ou para os já existentes e não incluídos no Manual de Controlo Interno, é da responsabilidade da equipa responsável por esse sistema ou tecnologia a identificação da exceção, devendo a mesma encontrar-se documentada e registada na CMDB ou em meio equivalente. Sempre que uma ação de renovação tecnológica não conduza ao cumprimento desta Política, deve ser mantida a identificação deste sistema como uma exceção documentada, salvaguardando que nenhuma alteração possa conduzir a uma situação de risco acrescido de segurança comparativamente à situação anteriormente em produção.

8.2 Sistemas e Tecnologias já existentes e incluídos no Manual de Controlo Interno

Para os Sistemas e Tecnologias já existentes e incluídos no Manual de Controlo Interno, em que se verifiquem situações nas quais a Política de Segurança não seja aplicável por razões técnicas e funcionais, as exceções devem ser documentadas e sujeitas a parecer da entidade responsável por esta Política, acompanhada de proposta de medidas que possam mitigar os riscos em causa.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 5.2 Information security roles and responsabulities.

9 Comunicação de Incidentes de Segurança

Sempre que seja identificada uma situação anómala que possa estar relacionada com a segurança lógica das TI, SI e REDE do MEO, esta deve ser imediatamente comunicada ao SOC/ CSIRT (Computer Security Incident Response Team) do MEO através dos seguintes pontos de contacto:

- Onedesk (canal Posto de Trabalho / Cibersegurança);
- Email: csirt@meo.pt
- Em caso de phishing poderá também ser utilizado o e-mail: phishing@meo.pt

A equipa do CSIRT deve tratar os incidentes por forma a minimizar o seu impacto para a organização, garantindo a segurança da informação..

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 6.8 Information security event reporting.

10 Revisão da Política de Segurança da Informação

10.1 Gestão dos Riscos da Organização

A Organização estabeleceu uma metodología de Identificação e Avaliação de Riscos para identificar e dar resposta aos riscos que se colocam à segurança dos sistemas de rede e informação. São realizadas e documentadas avaliações dos riscos sendo aplicados os respetivos planos de tratamento de riscos. Os resultados da avaliação dos riscos e os riscos residuais são aprovados pela Gestão de Topo ou, quando aplicável, pelas pessoas responsáveis e com autoridade para gerir os riscos.

10.2 Gestão dos Riscos na Cadeia de Fornecimento

A organização estabeleceu uma Política de Compras, onde asume a importância da cadeia de fornecedores como componente determinante para concretizar a estratégia de negócio. Esta Política aplica-se internamente a todos os colaboradores, que direta ou indiretamente estejam envolvidos em atividades de contratação de fornecedores, nas empresas do Grupo e externamente a todos os fornecedores e aos seus colaboradores, assim como às empresas que estes venham a subcontratar.

No âmbito da monitorização e acompanhamento a organização reserva-se no direito de avaliar o cumprimento dos principios aceites pelos fornecedores, através de atividades de verificação, como pedidos de resposta a questionários (Self Assement Audit) ou visitas aos locais de desenvolvimento da atividade.

Os critérios de avaliação considerados podem abranger temas como proatividade e inovação, o cumprimento dos prazos acordados, a qualidade do serviço, os tempos e qualidade de resposta a solicitações, o cumprimento de requisitos de segurança de informação, critérios ambientais, sociais e de governança (ESG), cumprimento de normativos éticos e de conduta, entre outros que se venham a considerar pertinentes

11 Diretrizes de Segurança da Informação aplicáveis à utilização de Inteligência Artificial

A organização cumpre com os requisitos legais e regulamentares atualmente em vigor. É consentida a utilização de inteligência artificial devidamente autorizada pela organização. Caso contrário, aplica-se o Ponto 8 (Exceções e Pareceres à Política de Segurança da Informação) da Política de Segurança da Informação do Grupo MEO.

12 Revisão da Política de Segurança da Informação

A Política de Segurança da Informação é revista anualmente, sempre que ocorram incidentes significativos ou alterações significativas das operações ou dos riscos, decorrente de alterações na legislação e regulação aplicável, na estratégia de negócio e no perfil de risco do Grupo MEO.

As alterações a esta política são aprovadas pelo Gestão de Topo do Grupo MEO, sendo a nova versão publicada e divulgada a todos os colaboradores e entidades terceiras envolvidas nas atividades do Grupo MEO.

ISO / IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.1 Policies for information security

A presente Política foi aprovada em reunião de Comissão Executiva do dia 03/10/2025, de acordo com a Ordem de Serviço 3/2025.

13 Glossário

A

Audit Trail – Log que de uma forma cronológica regista a sequência de eventos auditáveis, contendo evidência da execução de transações ou funções de sistema. O mesmo deve conter informação relativa a: "Quem fez?"; "Quando fez?"; "Como Fez?", "De onde Fez?"; "O que Fez?"; "Porque Fez?", devendo guardar o valor/ parâmetro anterior e novo.

API - Application Programming Interface

Ativo - todos os Configuration Item necessários às prestações de serviços contratados, nomeadamente servidores, routers, firewalls, switchs, bases de dados, Sistemas Operativos, etc.

B

Base de dados – Conjunto de dados logicamente ligados entre si, num suporte que permite armazenamento de grande quantidade dos dados e geridos por um programa especializado denominado Sistema de Gestão de Bases de Dados. Este programa encarrega-se de armazenar e pesquisar os dados, garante independência entre a estrutura de armazenamento e outros programas que utilizam os dados, garante a segurança no acesso aos mesmos e assegura redundância e tolerância a falhas dos programas de consulta.

BSS – Business Support Systems.

C

Cifrar (Encryption) – Processo que envolve a codificação de dados de forma a garantir a confidencialidade, autenticidade, anonimato, time- stamping (registo do tempo de criação e modificação de um documento) e outros objetivos de segurança.

Cyber Hygiene - A ciber higiene diz respeito aos cuidados básicos de caráter preventivo de segurança no ciberespaço. Uma boa ciber higiene reduz a oportunidade de sucesso para ciberataques. Envolve tipicamente os seguintes vetores de boas práticas técnicas: 1) eliminação contínua de vulnerabilidades conhecidas de segurança nos diferentes ativos (p.e., via upgrades, security hardening, patching, atualização de certificados digitais, fecho de portas IP indevidamente abertas, atualização de anti-virus, …), 2) correção rápida de sistemas comprometidos (p.e., por malware) e eliminação das suas causas primárias, 3) gestão estrita de acessos com privilégios de administração e de acessos de risco à Internet, e, finalmente, 4) gestão dos inventários (e.g, CMDB) e do software autorizado.

CMDB – Configuration Management Database

Chain letters - Message sent to several people, requesting of each one to forward copies to their contacts and friends, and it may in certain situations refer to a threat that something ominous might happen if the message is not forwarded.

Controlo de Acessos – Sistema que restringe as atividades dos Utilizadores e processos baseado no que é estritamente necessário saber/fazer. Permite implementar a segregação de funções.

D

Dado – Representação de um facto, medição, conceito ou ideia através da utilização de letras, números, caracteres especiais, imagens ou sons, armazenado num computador permitindo a sua posterior consulta, transmissão ou processamento usando meios informáticos.

Dados Pessoais – Informação relativa a uma pessoa singular identificada ou identificável (titular dos dados); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da sua identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular (RGPD, art.º 4, n.º 1).

Dados pessoais sensíveis – são os que estão sujeitos a condições de tratamento especial, nomeadamente origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a um indivíduo.

Dados Críticos - São considerados dados críticos todos os números, índices, documentos e relatórios confidenciais que têm relação direta com os serviços prestados ou com os produtos vendidos por uma empresa. Tratam-se de informações que são essenciais para o funcionamento da empresa.

Data Center ou salas técnicas do tipo ANG (Áreas de Nova Geração) – Local com as condições ambientais e técnicas, (incluindo de segurança física e lógica, adequadas ao alojamento de equipamentos / sistemas, com um rigoroso controlo de acessos físicos e lógicos.

DMZ (Demilitarized Zone) – É um perímetro de segurança físico ou lógico utilizado para colocar front-ends dos serviços da empresa que se pretendem expor a um maior e não necessariamente confiável público-alvo, normalmente na Internet.

DoS (Denial of Service) and DDoS (Distributed Denial of Service) – Tipo de ataque a um sistema de informação ou rede com a intenção de provocar indisponibilidade do serviço

aos restantes Utilizadores, normalmente através da perda de conectividade e serviços pelo consumo agressivo da largura de banda da rede atacada ou de sobrecarga dos recursos dos sistemas atacados. Designa- se DDoS quando o ataque envolve múltiplos sistemas, distribuídos na Internet.

E

Estação de Desenvolvimento (TD) – Computador pessoal, fixo e ou portátil, e respetivo software, disponibilizado pelo MEO a um grupo restrito de Utilizadores, para uso profissional no MEO, ficando estes com privilégios de administração local do equipamento.

Estação de Trabalho (ET) – Computador pessoal, virtual (VDi), fixo e ou portátil, e respetivo software, disponibilizado pelo MEO à maioria dos Utilizadores, para uso profissional no MEO, ficando estes sem qualquer privilégio de administração local do equipamento.

F

File Share Públicos, Privados – São espaços em disco, para partilha de ficheiros para um número restrito de Utilizadores (Privados), ou para toda a rede em que se encontram (Públicos).

Firewall – Barreira lógica que tem como objetivo impedir que Utilizadores ou processos acedam para além de um determinado ponto da rede, sem que tenham previamente passado uma validação de segurança (exemplo, fornecer uma password).

FTP – File Transfer Protocol

H

http/https – Protocolos de comunicação da World Wide Web, sendo o https a versão mais segura e recomendada para aplicações Web/Intranet envolvendo informação classificada;

I

IDS – Sistema de deteção de intrusões ou de tentativas de intrusão.

IPS (Intrusion Prevention System) – Sistema de prevenção de intrusões.

L

Load balancer – Técnicas, soluções ou arquiteturas equivalentes que permitem distribuir carga de trabalho pelos recursos em causa. Os recursos podem ser categorizados da seguinte forma: Storage, Rede ou CPU.

M

Malware – Refere toda a classe de software malicioso (vírus, spyware, worms, ...) desenhado para se infiltrar no computador, tirando partido de vulnerabilidades de segurança, sem o consentimento do Utilizador, e que normalmente tem objetivos ilícitos e nocivos.

N

Networking – Série de pontos ou nós (computadores, ativos de rede, impressoras, etc) interligados por um meio de comunicação (cabo de cobre, ótico, etc).

Network TAPs – Dispositivo de hardware que possibilita o acesso aos dados que passam na rede de comunicação entre computadores..

O

OSS – Operational Support Systems

P

Password default ou Password de "fábrica" – Password inicial atribuída quando um novo Utilizador é criado ou password inicial disponibilizada por um fornecedor de hardware/ software.

Plataforma de Serviços – plataformas técnicas que permitem a disponibilização de funcionalidades associadas à parametrização de qualquer tipo de serviços nas redes – cobre, fibra, etc (criar/ativar/desativar, controlar sessões, protocolos).

Protocolos Seguros – conjunto de regras standard para a comunicação segura de dados através de um canal de transporte

R

Remote Shell – um programa informático que permite aceder remotamente a outro computador. O recurso a remote shells terá lugar nos termos e requisitos estritos desta Política.

RFI – Request for Information

RFP – Request for Proposal – Consulta ao Mercado para obtenção de proposta técnica e comercial relativa a determinado Produto/Serviço.

Rede Wireless – Uma rede wireless (sem fios) é uma rede de computadores que não necessita de ligações por cabos – sejam eles telefónicos, coaxiais ou óticos — recorrendo a equipamentos que usam radiofrequência (comunicação via ondas de rádio) ou comunicação via infravermelho, como em dispositivos compatíveis com IrDA.

Router – Executa o roteamento do tráfego de rede. Os Core Router são routers que se encontram localizados nos backbone ou centros nevrálgicos da rede.

S

SCP – Secure Copy Protocol

SFTP – Secure File Transfer Protocol Sistema Crítico – Para efeitos desta Política, são considerados sistemas críticos os sistemas onde um acesso não autorizado, ou a execução de uma operação não autorizada, pode originar um impacto financeiro negativo na organização.

SMTP – Simple Mail Transport Protocol

SNMP – Simple Network Management Protocol

SpyWare and SpyWare Bots – Software infiltrado num computador que recolhe informação de uma organização ou pessoa sem o seu conhecimento e a transmite de um outro computador, normalmente na Internet. Um SpyWare Bot é um SpyWare mais sofisticado controlado por computadores remotos na Internet (Bot Controllers).

Spam – e-mail não solicitado primariamente com objetivos publicitários, enviado em grandes quantidades para indivíduos, listas, grupos, etc.

SSH – Secure Shell

Strong Authentication – Também designado TFA (Two-factor authentication) é um protocolo de autenticação que requer duas formas de autenticação para aceder a um sistema, em que a 1ª forma de autenticação corresponde a algo que o Utilizador conhece (p.e., um PIN ou uma password) e a 2ª forma corresponde a algo que o Utilizador possui (p.e., cartão magnético ou impressão digital).

T

TLS - Transport Layer Security

Túneis (Tunneling) – Tecnologia que permite encapsular pacotes de um protocolo em pacotes de um outro protocolo. Existem túneis para estabelecer comunicações mais seguras quando o protocolo envolvente permite encriptação. Existem também túneis criados para dissimular comunicações com protocolos proibidos numa organização encapsulando-os em protocolos comuns como https. Esta última utilização é estritamente proibida no Grupo MEO.

V

VDI (Virtual Desktop Infrastructure) – Estação de trabalho baseada num ecrã, teclado e rato mas estando o seu processamento entregue a uma máquina virtual que corre centralmente num servidor em ambiente de Data Center.

Virus – Programa que se replica, copiando-se para o código de outro programa, sistema de arranque do computador ou documento, e que normalmente persegue objetivos ilícitos e nocivos.

14 Anexo I – Objetivos do SGSI

O MEO definiu a seguinte estratégia que foi apresentada e partilhada com toda a organização:

- Centra-se em três eixos Investimento; Inovação; Qualidade de Serviço;
- Alicerça-se em: Proximidade, Intervenção Social junto dos nossos stakeholders internos e externos;
- Materializa-se em cinco pilares estratégicos: Qualidade de Serviço; Inovação; Pessoas; Marca; Sustentabilidade.

A estratégia encontra-se refletida em objetivos mapeados para o Sistema de Gestão de Segurança da Informação (SGSI) no sentido de assegurar uma gestão focada em resultados e na melhoria contínua assegurando a Qualidade de Serviço.

A Política de Segurança da Informação também se aplica ao Sistema de Gestão de Serviços (ISO20000), considerando assim os requisitos dos serviços.