Política Específica de Segurança da Informação para Infraestruturas

ÍNDICE

1. INTRODUÇÃO

A Política Específica de Segurança da Informação para Infraestruturas tem como objetivo complementar a Política de Segurança da Informação da Altice Portugal, no sentido de regular e implementar boas práticas de segurança e proteção da informação.

Esta Política Específica para Infraestruturas aplica-se a todos os Sistemas e utilizadores da rede interna da Altice Portugal – a ptNet. Este documento define as suas atribuições e regula o seu funcionamento, de forma a garantir os níveis adequados de segurança e proteção da Informação.

A Política Específica de Segurança da Informação para Infraestruturas aplica-se à camada de Infraestrutura que suporta as Tecnologias de Informação[1] e às Infraestruturas de Comunicações[2] da Altice Portugal.

2. ÂMBITO

Esta Política é aplicável a todos os colaboradores, fornecedores, prestadores de serviços, entidades externas que acedem às Tecnologias de Informação, Sistemas de Informação, Redes e Plataformas de Serviço da Altice Portugal.

No âmbito da ptNet, o termo "utilizador" será utilizado como referência a qualquer um dos indivíduos referidos anteriormente.

É indispensável assegurar que todos os utilizadores, independentemente do seu nível hierárquico, função e/ou vínculo contratual – internos à Altice Portugal ou empresas suas participadas ou afetos a entidades externas ou outros com quem a Altice Portugal contratou fornecimento de Produtos/Serviços – têm 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 e o cumprimento da integridade, confidencialidade e disponibilidade da informação.

Todo o acesso a informação, infraestrutura ou sistemas de informação que sejam propriedade da Altice Portugal, por parte de colaboradores externos ou parceiros, requer a pré-assinatura de Acordos de Confidencialidade (NDA – Non Disclosure Agreement), mesmo após o término da prestação do serviço.

[1] Qualquer combinação de dispositivos, equipamentos de rede, plataformas, processos, aplicações, interativos ou não, total ou parcialmente automatizados, que utilizem, armazenem, transportem ou transformem informação.
[2] Sistemas, equipamentos e elementos de rede que suportam os serviços de comunicações prestados pela Altice Portugal.

2.1. Exceções à Política

Todos os pedidos de exceção à Política Específica de Segurança da Informação para Infraestruturas da Altice Portugal têm que ser devidamente justificados, autorizados e documentados. Estes pedidos deverão ser enviados para a Direção de Cibersegurança.

2.2. Revisão da Política

A Política Especifica de Segurança da Informação para Infraestruturas é revista anualmente, ou sempre que se justifique em termos de necessidades técnicas ou de negócio.

3. DEVERES DOS UTILIZADORES

O universo de utilizadores ptNet é composto por todos os colaboradores do grupo Altice Portugal, colaboradores externos em regime de *outsourcing*, e ainda elementos externos à empresa com necessidade de acesso temporário (ex.: fornecedores, consultores e auditores). Os utilizadores da ptNet têm as seguintes responsabilidades no âmbito da segurança:

1. Zelar pelos equipamentos que lhes estão atribuídos, tanto de forma a garantir uma utilização no âmbito para que os equipamentos lhes foram atribuídos, como pela sua segurança (e da informação neles contida) e operacionalidade;

2. O cumprimento estrito da legislação relativa a direitos de autor é da estrita responsabilidade dos utilizadores. Não é permitido o uso de equipamentos periféricos de armazenamento de dados, tais como gravadores de CD's, discos USB ou similares, para cópia de programas informáticos, dados multimédia ou de qualquer outro documento que refira proteção de propriedade (*copyright*), nos termos em que essa cópia não seja autorizada;

3. Assegurar a confidencialidade das credenciais de acesso que lhes são confiadas;

4. Zelar pela segurança da informação da empresa, atribuindo-lhe a classificação apropriada quando sejam os donos da mesma e respeitando a classificação da informação a que têm acesso, procedendo em conformidade no seu manuseamento, no que diz respeito à sua confidencialidade e integridade. Se no cumprimento das suas atividades, os utilizadores da ptNet ficarem na posse de informações confidenciais ou proprietárias, estes devem garantir que as mesmas serão processadas com a maior confidencialidade, não as divulgando a terceiros;

5. Salvaguardar documentos (disponibilidade) relacionados com a atividade profissional do utilizador, armazenando-os nos servidores centrais, estando assim garantida a sua salvaguarda

através de processos de *backup*, bem como a segurança da informação em conformidade com os níveis de confidencialidade. Os processos automáticos de *backup* garantem a disponibilidade para reposição da informação armazenada nos servidores centrais, desde que a mesma esteja disponível para backup nos prazos definidos;

6. Apagar os documentos do utilizador dos servidores centrais cuja validade esteja excedida ou que já não sejam relevantes para o trabalho do utilizador ou para o negócio da Altice. Existem quotas de espaço em disco para armazenamento da informação, atribuídas por Direção ou grupo. As quotas poderão ser alteradas a pedido, carecendo de justificação por parte da Direção respetiva;
7. Os documentos de carácter pessoal deverão ser armazenados, exclusivamente, no computador do utilizador, em espaço devidamente identificável, não devendo o total de informação ser de tal maneira elevado que possa por em causa o desempenho dos equipamentos;
8. Os utilizadores são responsáveis por não ter comportamentos de risco (manuseamento do correio eletrónico, *malware*, navegação em websites perigosos, etc.) que coloquem em risco os sistemas ou informação da empresa. Têm ainda o dever de denunciar situações (ou suspeitas) anómalas que possam estar relacionadas com a segurança lógica das TI, SI ou rede da Altice Portugal.

4. ARQUITECTURA

É da responsabilidade da Direção de Engineering and Network:

- A arquitectura da infraestrutura de Rede e Segurança dos Datacenters;
- A definição de arquitetura da Rede WAN e LAN e respetiva gestão operacional.

A Direção de Engineering and Network é a entidade autorizada a efetuar pedidos aos fornecedores internos, relativos à infraestrutura de rede ou sistemas internos (ex.: sistemas/plataformas Telco), quer se trate de novas implementações, instalações, ligações, alterações, acessos, endereçamentos ou outros. No caso da infraestrutura computacional e dos sistemas de informação a entidade autorizada é a Direção de IT.

5. GESTÃO DOCUMENTAL

Para efeitos de Gestão Documental, será utilizado o repositório único de informação localizado no IBPMS, onde são asseguradas a disponibilidade e o controlo de acessos aos dados nele constante, conforme níveis de segurança pré-estabelecidos.

Este repositório deve obedecer a uma política de *Backups* regular (Políticas de Backup STANDARD) e os utilizadores nele definidos deverão obedecer às definições de Utilizador e Política de Passwords constantes deste documento, de forma a garantir os requisitos de disponibilidade, integridade e confidencialidade. Este repositório deve ainda garantir o *logging* dos acessos a todos os documentos nele constante e o controlo de versões (*versioning*).

6. GESTÃO DE ACESSOS

Os acessos especificamente contemplados nesta Política são:

- Acessos à ptNet (Rede Interna da Altice Portugal);
- Acessos remotos;
- Acessos locais.

Todos os acessos acima referidos deverão cumprir as orientações constantes na Política de Segurança da Informação, nomeadamente:

- Acessos inativos durante 60 dias (máximo) deverão ser bloqueados;
- Sempre que tecnicamente possível e sem impacto na rastreabilidade de utilizadores, no caso de estarem inativos durante 1 ano (máximo) deverão ser removidos;
- Acessos a Sistemas e Aplicações incluídas no Manual de Controlo Interno deverão ser objeto de revisão periódica, por parte dos responsáveis pelos acessos, no sentido de reavaliar a necessidade de manutenção dos mesmos;
- É obrigatória a execução de um procedimento que reavalie periodicamente a necessidade da manutenção de acessos privilegiados, contas com privilégios de administração em todas as tecnologias, sistemas e aplicações;
- São proibidos quaisquer acessos anónimos (ex.: *guest*);
- Todos os acessos requerem a existência de um procedimento de suporte aos pedidos de acesso e respetivas autorizações, referindo claramente de quem é a responsabilidade da aceitação dos pedidos, bem como do seu cancelamento.

6.1. Acesso à rede (interna) PTNET

Este tema foi considerado apenas para publicação interna da Organização.

6.2. Controlo de Acessos à Rede

Este tema foi considerado apenas para publicação interna da Organização.

6.3. Acessos Locais

Considera-se "Acesso Local" o acesso dentro do Datacenter a sistemas, plataformas ou infraestrutura. Os Acessos Locais podem ser atribuídos às equipas técnicas (colaboradores internos ou prestadores de serviços em regime de *outsourcing*) e ainda a clientes que tenham infraestrutura alojada em Datacenters da Altice Portugal. No caso do acesso local de clientes, as necessidades dependem dos serviços contratualizados e o acesso está restrito à sua infraestrutura e meios de acesso à mesma.

O acesso local (lógico) implica necessariamente permissões de acesso físico ao Datacenter em causa, de acordo com a política e procedimentos de acessos físicos.

Apenas são permitidos acessos locais a sistemas, plataformas ou infraestruturas quando devidamente justificados, e aprovados.

Existem as seguintes variantes relativamente à aprovação dos acessos locais:

- Colaboradores Internos da Altice Portugal ou empresas suas participadas - Aplicam-se as diretrizes descritas no capítulo 6.3 Acessos locais. Estes acessos são necessariamente nominais;
- Prestadores de serviços (colaboradores externos) - Aplicam-se as diretrizes descritas no capítulo 6.3 Acessos locais. Estes acessos podem ser atribuídos por prestador de serviços;
- Clientes - O acesso restringe-se às próprias infraestruturas e o nível do acesso deve estar contratualmente determinado e discriminado. Para além das diretrizes descritas no capítulo 6.3 Acessos locais, é necessária a discriminação, justificação e aprovação do cliente, de acordo com o especificado no respetivo contrato.

6.4. Controlos Automáticos e Reavaliação Periódica de Acessos

Deverão ser implementados controlos automáticos de bloqueio/eliminação de acessos sem utilização, e os procedimentos de reavaliação periódica de acessos G4.2.1_PO.0005 Diretivas para Pedido, Autorização Revisão de Acessos.

7. AUTENTICAÇÃO

Todos os sistemas de informação, infraestruturas e aplicações que necessitem de autenticação de utilizadores deverão autenticar centralmente na AD (Active Directory) de topo. Não são aceitáveis novas estruturas de gestão de *passwords* isoladas, com exceção dos casos que, por contingências da classificação de informação, obriguem a requisitos de segurança mais elevados, nomeadamente à utilização de mecanismos de autenticação forte.

Apenas serão aceites sistemas de autenticação complementares, nas seguintes situações:

- Quando a autenticação centralizada for inviável por questões técnicas;
- Em casos de incompatibilidade de determinados equipamentos.

Todos os eventos correspondentes a padrões anormais/suspeitos de autenticação devem ser enviados para a plataforma de correlação de eventos e monitorização do SOC.

8. SEGURANÇA NA RELAÇÃO COM FORNECEDORES

A relação com os nossos fornecedores pauta-se pelo cumprimento das diretrizes estabalecidas que têm como objetivo a proteção da informação da Altice Portugal acedida pelos fornecedores no âmbito da sua colaboração com a Altice Portugal, assim como a salvaguarda da integridade dos serviços prestados pela Altice Portugal. Assim, a gestão de fornecedores deve pautar-se pelas seguintes diretrizes:

- Acesso à Informação: o fornecedor obriga-se a aceder às informações da Altice Portugal e esclarecimentos que necessite sobre qualquer matéria da consulta e negociação, abstendo-se de qualquer uso indevido da mesma, respeitando os princípios estabelecidos na Política de Segurança da Informação;
- Desenho e integração de sistemas seguros: O fornecedor obriga-se a garantir que os processos de integração e desenvolvimento, no âmbito dos produtos e serviços fornecidos, respeitam os princípios estabelecidos na Política de Segurança da Informação;
- A Política de Segurança da Informação é disponibilizada aos fornecedores envolvidos nos processos de seleção para aquisição de produtos e/ou serviços no momento da emissão do Caderno de Encargos ou de outra informação relevante (ex.: RFI[3], RFQ[4]) no âmbito do processo de seleção;
- Os fornecedores envolvidos num processo de seleção para aquisição de produtos e/ou serviços, no qual o fornecedor tenha acesso a informação sensível, assinarão uma Declaração comprometendo-se com as condições gerais que constam no caderno de encargos que incluirão, entre outras, as vertentes da Confidencialidade e da Proteção de Dados;

[3] Request for Information
[4] Request for Quotation

- Sempre que se verifique, na relação da Altice Portugal com fornecedores, a necessidade de existência de suporte contratual ou instrumento legalmente equiparável, estes incluirão a obrigação de cumprimento da Política de Segurança da Informação, nomeadamente no que refere a confidencialidade da informação e obrigação de proteção de dados pessoais.

9. STANDARDS PARA DESENVOLVIMENTO DE APLICAÇÕES

Este tema foi considerado apenas para publicação interna da Organização.

10. LOGGING DE ATIVIDADES E/OU ACESSOS

De forma a salvaguardar contas de utilizadores e sistemas torna-se necessário, em situações de força maior, inspecionar e monitorizar atividades de comunicação na rede ou de atividade em determinados sistemas. Unicamente a Direção de IT e a Direção de Cibersegurança poderão executar ou delegar em terceiros a execução destas operações.

Preferencialmente, os *logs* deverão ser remetidos para um repositório centralizado sob gestão das equipas de administração respetivas. A totalidade ou apenas parte desta informação deverá ser enviada para a plataforma de correlação, que suporta a atividade do SOC (Security Operations Center) na identificação e despiste de incidentes de segurança (ver capitulo 17).

10.1. Requisitos de Logging

Os *logs* de atividades e/ou acessos deverão ser tão indeléveis quanto possível, ter retenção mínima de 30 dias, e incluir a seguinte informação mínima:

- Origem e destino de conexões (identificação de rede)
- Utilização de serviços
- Data e hora de acesso aos sistemas (*login* e *logout*)

Sempre que possível, os *logs* de atividades e/ou acessos deverão também conter:

- Alterações efetuadas ao nível de sistema
- Identificação do utilizador (*username*)

10.2. Logging de Acessos

Os acessos regulados nesta Política devem obedecer aos seguintes requisitos de *logging*:

- ptNet: *logging* centralizado;
- Acessos remotos: *logging* centralizado;

- Acessos locais: no próprio sistema e replicados para o *logging* centralizado.

10.3. *Logging* de plataformas, para cumprimento de requisitos legais

Devem ser estritamente garantidos os prazos de retenção para os diferentes tipos de informação, de acordo com a legislação a que a Altice Portugal está obrigada. São responsáveis pela disponibilidade e integridade dos dados supracitados os administradores das plataformas respetivas (ex.: RADIUS Telepac, RADIUS Prime, plataformas de mail, portal SAPO, etc.).

O âmbito desta secção abrange quaisquer plataformas que possibilitem, a um utilizador ou cliente Altice Portugal, acesso à Internet com endereço IP público da responsabilidade da Altice Portugal – todos estes acessos deverão ser objeto de *accounting*, sendo os registos conservados durante o período de retenção obrigatório por lei ou descritos em Ordem de Serviço (OS32010CAPTP).

11. EVENTOS DE SEGURANÇA

As Infraestruturas têm de gerar eventos de segurança inerentes, sendo necessário haver registo dos eventos, nomeadamente:

- Autenticação (ex.: início/fim de sessão, tentativas inválidas de autenticação, bloqueio de contas de utilizador);
- Controlo de Acessos (ex.: criação/remoção de contas de utilizador e perfis de acesso, acesso a objetos críticos, elevação de privilégios);
- Sistema (ex.: alteração de configurações, iniciar/reiniciar de serviços);
- Ataques (ex.: deteção/bloqueio de ataques de segurança);
- Rede (ex.: estado dos canais de comunicação, ligações ativas).

Os eventos gerados têm de registar, os seguintes atributos de informação:

- A data e hora do evento;
- O endereço IP do sistema que gerou o evento;
- Os portos e protocolos utilizados;
- O endereço IP do sistema afetado pelo evento;
- A identidade responsável pelo evento;
- A descrição do evento.

Os eventos de segurança têm de ser retidos pelo período mínimo de 1 ano.

12. ANTIVÍRUS

A existência de vírus (e *malware* em geral) em estações padrão e, principalmente em servidores, são vetores de ataque por excelência que colocam em risco a segurança da informação e dos sistemas. Para prevenir a receção de correio eletrónico contendo *malware*, todas as mensagens de correio eletrónico das plataformas de *e-mail* corporativas deverão ser inspecionadas por um sistema de deteção e remoção automática de vírus informáticos.

12.1. Gestão Centralizada de Antivírus

O Software de Antivírus, assim como as respetivas assinaturas serão atualizados automaticamente. No entanto, e dado o constante desenvolvimento de novos vírus associado à sua rápida disseminação, a eficácia deste tipo de deteção nem sempre pode ser garantida a 100%, razão pela qual poderão ser tomadas iniciativas destinadas ao combate a ameaças particulares que podem passar por medidas direcionadas ao tratamento de identificação ou remoção de *malware* (ex.: envio/aplicação urgente de *extradat* ou *pattern* de AV, limpeza local de *workstations* ou servidores, etc.).

12.1.1. Estação Padrão – Ambientes de colaboradores

As Estações Padrão têm que conter obrigatoriamente Software antivírus instalado, estando os utilizadores obrigados a permitir a atualização (centralizada) do mesmo.

12.1.2. Ambiente de IT

Os sistemas que suportam a infraestrutura tecnológica têm, sempre que o suportarem, de ter instalado uma ferramenta de deteção e limpeza de vírus. Deverão ainda existir as conectividades na rede interna que permitam a comunicação da plataforma centralizada de Antivírus com os sistemas.

Qualquer sistema cujo funcionamento esteja comprometido pela ação de um qualquer *malware* deverá avaliar a possibilidade de ser desconectado da infraestrutura para evitar posteriores desenvolvimentos que se reflitam negativamente sobre a mesma.

12.1.3. Ambiente de Cliente (em Data Center)

Os sistemas de clientes alojados em Datacenter da Altice Portugal deverão possuir ferramentas de deteção e limpeza de vírus. É recomendado um antivírus centralizado nos sistemas dos clientes.

Qualquer sistema cujo funcionamento esteja comprometido pela ação de um qualquer *malware* poderá ser desconectado da infraestrutura para evitar posteriores desenvolvimentos que se reflitam negativamente sobre a mesma ou sobre os serviços prestados. Nestes casos, o cliente deverá ser avisado,

pelo respetivo gestor, de qualquer alteração ou ação tomada sobre os seus sistemas ou de como afeta o seu serviço.

13. ANTI-SPAM

Por definição, considera-se SPAM qualquer mensagem eletrónica, não solicitada, enviada em massa com fins publicitários, para ataques de maliciosos denominados *phishing* quando se destinam a capturar informação do destinatário.

As plataformas Anti-SPAM permitem marcar e-mails de SPAM que são rececionados nas plataformas de *e-mail* (no sentido *inbound* da Internet para as plataformas de e-mail) podendo assim ser entregues em pasta criada para o efeito sem causar impactos.

Existem atualmente duas plataformas anti-SPAM, abrangendo os seguintes universos:

- *E-mail* corporativo (domínios do grupo Altice Portugal)
- Domínios de clientes Altice Portugal.

14. ATUALIZAÇÕES DE SOFTWARE

Em termos de impacto, a não instalação de atualizações de *software* relacionadas com segurança permite que uma ou várias vulnerabilidades, do domínio público, sejam exploradas para atacar (ex.: infetando com *malware*) os referidos Sistemas.

14.1. Sistemas

A instalação de *patch*es é da responsabilidade dos administradores de Sistemas das plataformas respetivas. Sempre que existam impedimentos técnicos que sustentem a não instalação de *patches*, as situações deverão ser consideradas exceções, e ser devidamente documentadas.

As atualizações deverão ser formalmente planeadas, de acordo com os procedimentos vigentes, que devem incluir o procedimento de *fall-back*.

No caso de sistemas de clientes, as atualizações requerem o acordo prévio do respetivo cliente. Qualquer sistema cujo funcionamento seja comprometido devido à não instalação de *patches* poderá ser desconectado da infraestrutura para evitar posteriores desenvolvimentos que se reflitam negativamente sobre a mesma ou sobre os serviços prestados. Nestes casos, o cliente deverá ser avisado, pelo respetivo gestor, de qualquer alteração ou ação tomada sobre os seus sistemas ou de como afeta o seu serviço.

14.2. Estações de Trabalho

A responsabilidade da distribuição de *patches* de segurança em estações de trabalho é das equipas de Desktop Management. A distribuição de atualizações de segurança realizada no âmbito de Desktop Management deverá acautelar o impacto na rede.

Recomenda-se a distribuição de atualizações fora do horário normal de trabalho ou ao fim-de-semana, ou ainda a distribuição faseada (por lotes de estações de trabalho).

15. SINCRONIZAÇÃO DE RELÓGIOS

Para se poder assegurar que todos os registos que incluem *timestamps* (ex.: *logs*, eventos a correlacionar, dados de tráfego, etc.) se referem ao mesmo referencial temporal, assegurando assim a validade legal dos mesmos, é imprescindível que todos os sistemas estejam sincronizados em termos de relógio por um referencial temporal único.

Assim, todos os sistemas têm obrigatoriamente que sincronizar os seus relógios pela plataforma de NTP (Network Time Protocol) centralizada.

Ao nível da segurança da plataforma centralizada NTP, recomenda-se:

- A utilização de uma topologia adequada e com o número suficiente de fontes de relógio que garantam a sua disponibilidade;
- Sempre que tecnicamente possível, a utilização de criptografia que garanta a autenticidade e integridade da informação de relógio disponibilizada aos diversos sistemas.

16. INCIDENTES DE SEGURANÇA

Entende-se genericamente como incidente de segurança, uma ação ou conjunto de ações desenvolvidas contra um computador ou rede de computadores que resulta, ou pode resultar, no comprometimento das propriedades básicas da segurança da informação: disponibilidade, integridade e confidencialidade.

Alinhadas com o processo de gestão de incidentes, devem ser utilizadas as designações específicas:

- Incidente de Segurança define-se como sendo uma violação ou ameaça iminente da Política de Segurança da Informação, das práticas de cibersegurança adotadas, originando uma indisponibilidade, degradação do serviço ou que poderá levar à sua indisponibilidade caso se mantenha o evento.
- Evento é o registo de qualquer ocorrência de cibersegurança observável num sistema ou rede.”

.

16.1. Classificação de Incidentes

É utilizada a classificação de incidentes estabelecida pelo CERT.PT e adotada pela Rede Nacional de CSIRTs, da qual a Altice Portugal é membro através do seu CSIRT. Esta classificação é baseada no resultado obtido ou pretendido com o ataque. http://www.cert.rcts.pt/images/docs/Taxonomiav2.5.pdf

16.2. Comunicação de Incidentes de Segurança

Sempre que seja identificada uma situação anómala e que possa estar relacionada com a segurança lógica das TI, SI ou rede da Altice Portugal (ex.: conhecimento de máquinas infetadas com *malware*, *e-mails* de *phishing* afetando a Altice Portugal ou a sua imagem, roubo de credenciais, etc.), esta deve ser imediatamente comunicada ao CSIRT da Altice Portugal (csirt@telecom.pt)

O contacto deverá ser efetuado através de *e-mail* para o CSIRT Altice Portugal ou poderá ser criado um ticket em Onedesk, 2.7 Cibersegurança, que o reencaminhará, após identificar o respetivo interlocutor.

A informação recebida é usada no tratamento do incidente respeitando as leis vigentes de privacidade e proteção de dados pessoais. A informação de dados pessoais não é libertada a terceiros e, em caso de real necessidade, é solicitada à pessoa/entidade relatora uma autorização expressa para o efeito.

17. Security Operations Center (SOC)

O SOC é uma equipa centralizada na Altice Portugal, especializada em Segurança de Sistemas de Informação, responsável pela deteção e resposta a incidentes de Segurança.

Os sistemas, plataformas e tecnologias críticas para o negócio da Altice Portugal, deverão estar sob a monitorização do SOC.

Adicionalmente, os eventos gerados por tecnologias de deteção de vulnerabilidades de segurança lógica, sistemas de deteção de intrusão, antivírus, *firewalls* e plataforma de autenticação centralizada, deverão ser enviados para a plataforma de correlação de eventos e monitoria do SOC.

18. NORMAS DE CONFIGURAÇÃO DO SISTEMA OPERATIVO

Os seguintes procedimentos gerais de instalação devem ser seguidos para todas as implementações do sistema:

1. Se a máquina for uma nova instalação, deve ser protegida do tráfego de rede hostil até o sistema operacional ser instalado e robustizado (*hardened*):
2. Instalação do sistema operativo;
3. Atualização de todos os *softwares* do sistema operacional de acordo com as recomendações do fornecedor;
4. Configurar os parâmetros do sistema operacional de acordo com CIS Benchmarks (OS *hardening*).

18.1. Sistemas Windows

Os seguintes procedimentos de instalação e configuração devem ser seguidos para todas as implementações do sistema baseadas no Windows.

Step	Action	CIS Benchmark Reference
	Preparação e Instalação	
1	Se a máquina for uma nova instalação, deve ser protegida do tráfego de rede hostil até o sistema operacional ser instalado e hardened	
2	Consider using the Security Configuration Wizard to assist in hardening the host	
	Packs de Serviço e Hotfixes	
3	Install the latest service packs and hotfixes from Microsoft	
4	Enable automatic notification of patch availability	
	Políticas de contas de utilizador	
5	Set minimum password length	1.1.4
6	Enable password complexity requirements	1.1.5
7	Do not store passwords using reversible encryption	1.1.6
8	Configure account lockout period	1.2
	Atribuição de Direitos de Utilizador	
9	Restrict the ability to access this computer from the network to Administrators and Authenticated users	2.2.2
10	Do not grant any users the ‘act as part of the operating system’ right	2.2.3
11	Restrict local logon access to Administrators	2.2.6
12	Deny guest accounts the ability to logon as a service, a batch job, locally or via	2.2.18-21

	RDP.	
	Configurações de Segurança	
13	Disallow users from creating and logging in with Microsoft Accounts	2.3.1.1
14	Disable the guest account (default)	2.3.1.2
15	Require Ctrl-Alt-Del for interactive logins (default)	2.3.7.2
16	Configure machine inactivity limit to protect idle interactive sessions	2.3.7.3
17	Configure MS Network Client to always digitally sign communications	2.3.8.1-2
18	Disable the sending of unencrypted passwords to third party SMB servers	2.3.8.3
19	Configure MS Network server to always digitally sign communications	2.3.9.2-3
	Controlos de Acesso à Rede	
20	Disable anonymous SID/Name translation (default)	2.3.11.1
21	Do not allow anonymous enumeration of SAM accounts and shares	2.3.11.2-3
22	Do not allow Everyone permissions to apply to anonymous users (default)	2.3.11.4
23	Do not allow any named pipes to be accessed anonymously.	2.3.11.5
24	Restrict anonymous access to named pipes and shares (default)	2.3.11.8
25	Do not allow any shares to be accessed anonymously	2.3.11.9
26	Require the "Classic" sharing and security model for local accounts (default)	2.3.11.10
	Configurações de Segurança de Rede	
27	Allow Local System to use computer identity for NTLM	2.3.12.1
28	Disable Local System NULL session fallback	2.3.12.2
29	Configure allowable encryption types for Kerberos	2.3.12.4
30	Do not store LAN Manager hash values	2.3.12.5
31	Set LAN Manager authentication level to only allow NTLMv2 and refuse LM and NTLM	2.3.12.7
32	Enable the Windows Firewall in all profiles (domain, private, public) (default)	9.[1-3].1
33	Configure the Windows Firewall in all profiles to block inbound traffic by default (default)	9.[1-3].2
	Active Directory Domain Member Security Settings **Configurações de Segurança do Responsável de Domínio do Active Directory**	
34	Digitally encrypt or sign secure channel data (always) (default)	2.3.6.1
35	Digitally encrypt secure channel data (when possible) (default)	2.3.6.2
36	Digitally sign secure channel data (when possible) (default)	2.3.6.3
37	Require strong (Windows 2000 or later) session keys	2.3.6.6
38	Configure the number of previous logons to cache	2.3.7.6
	Configurações da Audit Policy	
39	Configure Account Logon audit policy	17.1
40	Configure Account Management audit policy	17.2
41	Configure Logon/Logoff audit policy	17.5
42	Configure Policy Change audit policy	17.7
43	Configure Privilege Use audit policy	17.8
	Configurações do Event Log	
44	Configure Event Log retention method and size	18.7.19
45	Configure log shipping for centralized logging (e.g. to Splunk)	

	Proteção de Segurança Adicional	
46	Disable or uninstall unused services	
47	Disable or delete unused users	
48	Configure User Rights to be as secure as possible	
49	Ensure all volumes are using the NTFS file system	
50	Configure file system permissions	
51	Configure registry permissions	
52	Disallow remote registry access if not required	2.3.11.6
	Passos Adicionais	
53	Set the system date/time and configure it to synchronize against campus time servers	
54	Install and enable anti-virus software	
55	Install and enable anti-spyware software	
56	Configure anti-virus software to update daily	
57	Configure anti-spyware software to update daily	
58	Install software to check the integrity of critical operating system files	
59	If RDP is utilized, set RDP connection encryption level to high	
60	Install EMET	18.7.17
	Segurança física	
61	Set a BIOS/firmware password to prevent alterations in system start up settings	
62	Disable automatic administrative logon to recovery console	2.3.13.1
63	Do not allow the system to be shut down without having to log on	2.3.14.1
64	Configure the device boot order to prevent unauthorized booting from alternate media	
65	Configure a screen-saver to lock the console's screen automatically if the host is left unattended	

Verificar junto de https://benchmarks.cisecurity.org/tools2 os mais recentes guias de configuração.

18.2. Sistemas Linux

Os seguintes procedimentos de instalação e configuração devem ser seguidos para todas as implantações do sistema baseadas no Linux

1. Se a máquina for uma nova instalação, deve ser protegida do tráfego de rede hostil até o sistema operacional ser instalado e *hardened*:
2. Instalação do sistema operativo;
3. Atualização de todos os *softwares* do sistema operacional de acordo com as recomendações do fornecedor;
4. Configurar os parâmetros do sistema operacional de acordo com CIS Benchmarks (OS *hardening*) incluindo:

a. Desativar todos os serviços não utilizados
b. Desativar serviços não seguros como o telnet e FTP e instalar serviços seguros equivalentes (SSH, SFTP)
c. Desativar *logins* remotos para *root*
d. Instalar GR Security
e. Configurar *log shipping* para *logging* centralizado (ex.: Splunk)
f. Instalar um File Integrity Monitor ou Host-IDS (ex.: OSSEC)
g. Evitar executar serviços como *root*

5. Segurança física:
    a. Definir uma *password* BIOS/*firmware* para evitar alterações nas configurações no arranque do sistema
    b. Configurar a ordem de *boot* do dispositivo para evitar o *booting* não autorizado a partir de média alternativa
    c. Configurar o *screen-saver* para bloqueio automático do ecrã quando este for deixado sem vigilância

Verificar junto de https://benchmarks.cisecurity.org/tools2 os mais recentes guias de configuração.