TERMOS E CONDIÇÕES DE UTILIZAÇÃO DA REDE INFORMÁTCIA IPT

1.0 Finalidade deste Documento

Esta política foi concebida para proteger a rede do campus do Instituto Politécnico de Tomar adiante designado por IPT, e para garantir que os seus utilizadores a usam de forma eficiente e segura.
O objetivo desta política é também definir regras para que quaisquer dispositivos que se liguem à rede do IPT, o façam de forma considerada segura e não interferente.
As regras foram definidas para minimizar a exposição da comunidade do IPT a riscos que sejam considerados, pelo Centro de Informática e Sistemas adiante designado por CIS, como elevados e de forma a minimizar as perturbações laborais e as perdas de dados que possam resultar de computadores e servidores que não são configurados ou mantidos corretamente, e também para garantir que os dispositivos dos utilizadores se liguem sem realizar ações que possam prejudicar o desempenho da rede.

O Politécnico de Tomar deve fornecer uma rede segura para necessidades e serviços de investigação, desenvolvimento, educação, formação e funcionamento dos seus serviços adjacentes e coadjuvantes. Um computador não seguro na rede permite ataques que bloqueiam serviços, que circulem vírus e trojans, bem como outros tipos de tentativas de intrusão a dispositivos que existam e residam no campus, afetando muitos outros dispositivos de rede e a consequente produtividade, bem como a integridade da infraestrutura de rede e respetivos serviços. Os danos causados por explorações mal intencionadas podem incluir a perda de dados confidenciais e não confidenciais, interrupção de serviços de rede e danos nos sistemas críticos. As instituições de ensino que sofreram ataques graves também sofreram danos na sua imagem pública, portanto, os indivíduos que liguem os seus dispositivos, servidores e outros tipos equipamentos à rede devem seguir procedimentos específicos e tomar as precauções adequadas antes de serem ligados.

2.0 Abrangência

Esta política aplica-se a todos os membros da comunidade do Politécnico de Tomar ou a visitantes que possuem algum tipo de dispositivo que pretendam ligar na rede, incluindo, entre outros, computadores desktop, laptops, servidores, computadores sem fio, dispositivos móveis, smartphones, equipamentos especializados, câmeras, sistemas de controle acessos e ambiental e componentes do sistema telefónico. A política também se aplica a qualquer pessoa que tenha sistemas fora da rede do campus mas que aceda à rede e aos recursos existentes no campus. A política aplica-se a computadores pertencentes ao Politécnico e a computadores pessoais que se liguem à rede.

3.0 Política de Acesso

3.1 Métodos de ligação apropriados

Podem ser ligados dispositivos à rede do campus em pontos de rede com e sem fios, incluindo tomadas físicas e pontos de acesso de rede sem fios geridos ou aprovados pelo centro de informática e sistemas, através de túneis VPN ou SSH ou desktop remoto ou através de outros mecanismos de acesso remoto tais como modems xdsl e modems tradicionais de telefone de linhas fixas ou móveis.
A introdução de equipamentos de comutação complementar na rede ou as suas modificações podem causar efeitos indesejáveis, tal como, perda de conectividade. Esses efeitos nem sempre são imediatos e nem sempre essas alterações são registadas, adicionadas ou comunicadas ao CIS. Como resultado, a extensão ou modificação da infraestrutura de rede deve ser feita segundo as regras publicadas pelo CIS, excepções serão abertas para as redes e servidores geridos pelos departamentos ou docentes que possuam competências naqueles equipamentos. As regras pelas quais se regem este tipo de circunstâncias serão as de entrega de conectividade para acesso ou de gestão de servidores.

3.2 Acesso à rede

Os Utilizadores da rede do IPT têm sempre de se autenticar para conseguir ligar um dispositivo da rede.
O CIS mantém uma base de dados com as identificações das máquinas, endereço de rede e o utilizador que neles se ligaram e dos acessos entregues, para que no caso de haver algum tipo de infração que configure a violação da lei, facilmente, o dono do dispositivo possa ser contactado. Por exemplo, o CIS entraria em contato por email com o dono de um dispositivo no caso de este se encontrar comprometido ou se já estiver iniciado algum tipo de ataque ou se esteve sujeito à emissão de um aviso de violação de direitos autor para o endereço IP usado por esse dispositivo.

3.3 Responsabilidade pela segurança

Todo o computador ou outro tipo de dispositivo ligado na rede, seja um computador portátil ou outro tipo de dispositivo qualquer, tem um dono associado ou um Resposável. De modo a facilitar a redação desta politica, os donos e reponsáveis por dispositivos são referidos como donos.
Os donos são responsáveis por garantir que os seus dispositivos respeitem as regras de segurança mais relevantes e que configurem a segurança do

equipamento e dos serviços que neles funcionam. Alguns departamentos podem atribuir a responsabilidade da segurança e manutenção dos computadores a terceiros, sendo possível que um dono possa gerir vários dispositivos, incluíndo os seus dispositivos pessoais.
Todo dono deve saber quem é o responsável pel manutenção e bom funcionamento das seu(s) dispositivo(s).

3.4 Segurança

As regras de segurança aplicam-se a todos os dispositivos que se liguem à rede do politécnico através de pontos de ligação fixos e sem fios bem como de ligações com origem exterior ao campus.
Todos os donos devem garantir que todos os computadores e outros dispositivos capazes de executar software anti-vírus e anti-malware tenham esses softwares actualizados, instalados e em execução.
Os donos de computadores que neles guardem informações sensiveis, confidenciais ou com outro tipo de restrição pública devem aplicar proteções extras. A equipa do CIS indicará medidas, a pedido dos donos de computadores, que gostariam de mais informações sobre medidas extra de segurança e que possam ser tomadas por forma a que os equipamentos fiquem protegidos de forma adquada.

3.5 Serviços baseados em rede com serviços centralizados

O CIS, é responsável por fornecer serviços de rede confiáveis para todo o campus. Como tal, indivíduos ou departamentos não podem executar nenhum serviço que
perturbe ou interfira com os serviços prestados centralmente. Esses serviços incluem, mas não estão limitados a, e-mail, DNS, DHCP, HTTPS e HTTP. Excepções serão feitas para as redes, serviços e servidores geridos pelos departamentos ou docentes que possuam competências naqueles equipamentos e na gestão dos serviços acima mencionados.
OS indivíduos ou departamentos que se enquadrem na excepção anterior não podem executar nenhum serviço ou configurar um servidor que solicite a um
indivíduo o binómio utilizador/password de forma não federada, simples ou direta ou cujos serviços conflituem ou se sobreponham aos serviços geridos pelo CIS.

3.6 Proteção da Rede

O CIS usa vários métodos para proteger a rede, entre os quais, a monitorização de intrusões e o Rastreio de dispositivos na rede para averiguar a possivel existência de anomalias suspeitas ou de tráfego considerado nocivo.

Todo o tráfego de rede que passa dentro ou fora da infraestrutura é monitorizado por um sistema de detecção de intrusão ou de análise de URL's e URI´s.
Ao ligar um computador ou dispositivo à rede, o utilizador está a reconhecer que o tráfego da rede para e do seu computador pode ser analizado e registado.
O CIS, rotineiramente, efetua varrimentos em busca de vulnerabilidades, logo, ao ligar-se à rede o utilizador concorda que o seu computador ou dispositivo possa ficar sujeito a análises para que sejam identificadas possíveis vulnerabilidades.
O CIS reserva-se no direito de tomar as medidas necessárias para conter problemas de segurança ou tráfego de rede incomum. O CIS, tomará medidas para conter dispositivos que exibam os comportamentos indicados abaixo e que não permitam que o tráfego flua e que os serviços sejam usados de forma normal.

- Colocando cargas de tráfego que provoque a interrupção do funcionamento ou forneciemnto normal de um serviço ou mais serviços de rede do campus.
- Colocando cargas de tráfego que provoque a interrupção do funcionamento ou forneciemnto normal de serviços prestados centralmente.
- Exibindo padrões de tráfego de rede consistente com tráfego malicioso ou a uma infecção por rootkit ou outro tipo de ameaças.
- Exibindo um comportamento consistente com uma infeção por virus ou por malware.
- O CIS reserva-se o direito de restringir certos tipos de tráfego que transita pela rede.
- O CIS reserva-se no direito de restringir o tráfego que é conhecido por causar danos a estruturas de rede e aos dispositivos que nela se encontram ligados, por exemplo, o NETBIOS.
- O CIS também pode controlar outros tipos de tráfego que são conhecidos pelo seu consumo excessivo de tráfego de rede, exemplo, partilha de ficheiros que não sejam considerados legais em P2P.

Ao ligar-se à rede, o dono do dispositivo aceita que um computador ou outro dispositivo que exiba qualquer um dos comportamentos acima indicados seja considerado como estando a incorrer na violação desta política. Posteriormente, será avisado, e poderá o seu acesso ou o dispositivo(s) ficar bloqueado na rede até que apresente um comportamento em conformidade.

3.7. Utilização da conta do IPT

As contas atribuídas aos utilizadores são propriedade do Politécnico de Tomar e só poderão usufruir de uma conta os indivíduos que sejam alunos, docentes, funcionários ou colaboradores do politécnico de Tomar.
Os utilizadores ficam também informados de que a sua conta é pessoal e intransmissivel, não podendo ceder a sua utilização a terceiros. Deve procurar evitar que a sua conta não seja um meio de propagação de todo e qualquer tipo de 'Spam', 'hoax', 'phishing', 'worms' e 'worms enviados massivaemnte por email', bem como, deve evitar deixar as sessões abertas em computadores partilhados/públicos, utilizar

uma password segura mas com preferencia para a utilização de uma passphase que devem ser alteradas com alguma regularidade e que não devem ser transmitidas a terceiros.

4. Termos de Aceitação

A aceitação desta politica implica que o utilizador tenha conhecimento da lei do Cibercrime (Lei nº109/2009 de 15 de Setembro), nomeadmente no seu capítulo II do seu artigo 3º ao seu artigo 8º e que se comprometa sob compromisso de honra a respeitar todas as disposições nela contidas bem como respeitar todos os pontos que definem esta política.