Normas de gestão
da rede informática
do Instituto Superior Técnico

CIIST - Centro de Informática do Instituto Superior Técnico

V 1.2 - Setembro de 2007

Instituto Superior Técnico

Setembro de 2007

Resumo

Este documento estabelece normas gerais de gestão da rede do IST que deverão ser adoptados por todos os responsáveis administrativos e técnicos da rede informática do IST. Pretende-se, deste modo, estabelecer um conjunto de regras que contribuam para uma maior segurança e uma maior consistência de procedimentos na gestão rede do IST, contribuindo assim para o aumento da qualidade de serviço.

Índice

Capítulo 1

Introdução

1.1 Enquadramento

Durante vários anos, a gestão da rede do IST baseou-se num modelo fortemente descentralizado, em que os serviços do CIIST, além de albergarem os serviços centrais, limitavam-se a fornecer conectividade aos diversos centros de investigação e Departamentos do IST. Durante este período, do ponto de vista de gestão de rede, o papel do CIIST limitou-se essencialmente à regulamentação da divisão do espaço de endereçamento, gestão e administração do *backbone* de rede, conectividade com o exterior e manutenção da rede administrativa.

Este modelo de desenvolvimento descentralizado resultou da combinação dois factores fundamentais:

- Rápida expansão da rede, com consequente dificuldade por parte do CIIST em acompanhar as necessidades imediatas de Departamentos e Centros de Investigação.
- Existência de competências técnicas em vários Departamentos e Centros de Investigação capazes de usar os seus recursos próprios para realizar a gestão das suas redes locais.

Apesar de sempre terem existido problemas de segurança na Internet, o número de ameaças reais durante esta fase inicial foi moderado, dado que a maioria das instituições ligadas eram académica e de investigação. A situação altera-se durante a década de 90 com a entrada em cena dos primeiros servidores público de Internet (ISP's) e a consequente expansão da Internet entre utilizadores comerciais e particulares. A partir desta altura, o número de ameaças à segurança e bom funcionamento da Internet cresce significativamente, levando a que várias instituições come-

cem a impor regulamentações mais restritas de acesso à rede e sistemas de segurança que possam lidar com o novo modelo de exploração da Internet, enquanto rede global de acesso livre. Este cenário veio também aumentar o nível responsabilidade civil e criminal a que estão sujeitas as diversas entidades utilizadoras da Internet, sobretudo quando a sua rede é utilizada, ainda que involuntariamente, como base para ataques de segurança a outras redes.

Actualmente, para além das ameaças de segurança directa, o crescimento explosivo de mail não solicitado (*spam*), acompanhado da profusão de vírus e *worms*, conduziram a uma situação em que a gestão de redes informáticas exige elevado rigor técnico, dedicação permanente e constante actualização dos administradores de rede. Por outras palavras, esta realidade não é compatível com modelos de administração baseados apenas em curiosidade técnica ou na simples existência de bons conhecimentos técnicos sobre redes e servidores. Neste quadro, torna-se conveniente definir um conjunto de regras para a gestão da rede do IST e que possam ser adoptadas por Grupos de Investigação e Departamentos como referência na gestão e acesso à rede do IST.

Uma parte das regras aqui enunciadas corresponde apenas a simples normas de bom senso ou a regulamentos *ad-hoc* informalmente já discutidos e aceites na lista de mail IST-sysadm. Espera-se, com este documento, centralizar e sistematizar estas regras, de modo a que passem a fazer parte da prática comum de todos os envolvidos na gestão da rede do IST.

1.2 Objectivos

Pretende-se com este documento:

- Estabelecer as regras as administrativas que devem ser adoptadas por Departamentos e Centros de investigação que mantenham sistemas próprios de gestão das suas sub redes e máquinas.
- Estabelecer um conjunto de normas técnicas a serem adoptadas por todos os administradores de sub-redes do IST de modo a melhorar a gestão da rede.

Este documento é aberto, esperando-se que, venha a evoluir com as criticas e sugestões que sejam formuladas.

1.3 Convenções

Este documento inclui, para além do texto de enquadramento, normas, recomendações, sugestões e informações. Neste contexto, deverão ser consideradas as seguintes definições:

Normas Princípios regulamentares que deverão ser considerados obrigatórios na administração e gestão da rede do IST.

Recomendações Princípios regulamentares que deverão ser tendencialmente implementados na totalidade da rede do IST e que deverão ser obrigatoriamente considerados na implementação ou configuração de novos sistemas.

Sugestões Indicações gerais, de carácter não obrigatório, mas cujo adopção se considera aconselhável.

Informações Pontos informativos importantes.

Para maior destaque, normas, recomendações, sugestões e informações serão sempre apresentadas sob a forma de listas de itens. Para diferenciação, utilizar-se-á a seguinte anotação:

- (N) - Identificação de **normas**.
- (R) - Identificação de **recomendações**.
- (S) - Identificação de **sugestões**.
- (I) - Identificação de **informações**.

1.4 Estrutura

No capítulo 2 definem-se normas administrativas que deverão seguidas pelos Departamentos e Centros de Investigação para garantir uma boa articulação com os serviços centrais do CIIST. No capítulo 3 referem-se um conjunto de procedimentos e normas técnicas que deverão ser adoptados pelos administradores das sub-redes do IST. No capítulo 4 referem-se as políticas de utilização da rede do IST e normas a adoptar em casos específicos. Finalmente, no capítulo 5, refere-se a validade deste documento e mecanismos previstos para a sua revisão.

Capítulo 2

Normas Administrativas

2.1 Introdução

Por razões históricas, a responsabilidade de gestão da rede do IST tem sido partilhada entre o CIIST e os vários Centros e Departamentos do IST.

De uma forma geral, o CIIST tem sido responsável pelo *backbone* de rede, servidores centrais e máquinas dos serviços administrativos. As máquinas e redes internas dos departamentos e centros de investigação são responsabilidade dessas entidades. Neste contexto, entende-se por *backbone de rede* todo o sistema de encaminhamento, entrega e distribuição de tráfego nos diversos edifícios e centros do IST. Em cada edifício o *backbone* de rede pode é geralmente constituído por um ou mais bastidores com equipamentos activo e a cablagem de interligação ao *routers* centrais (os limites exactos do *backbone* são variáveis e dependentes do edifício / local, devendo ser estabelecidos de comum acordo entre o CIIST e as entidades interligadas).

Como já foi referido, anteriormente, a existência de uma responsabilidade distribuída reforça a necessidade de serem estabelecidadas regras que permitam a coerência e segurança da globalidade da rede.

2.2 Responsabilidade administrativa

- (N) Todos os computadores ligados à rede do IST e sub-redes locais dos Departamentos e Grupos ou Institutos de Investigação deverão ter um responsável administrativo claramente estabelecido.

Como norma, o responsável administrativo deverá ser o responsável pelo Departamento, Grupo ou Instituto de Investigação em que a máquina e sub-rede local em que a máquina está inserida ou o elemento em quem este delegue esta responsabilidade.

- (R) O responsável administrativo deverá ser um Docente ou Investigador do Departamento ou Grupo de Investigação, a quem competirá:
  - Definir a política de utilização e acesso à máquina.
  - Servir de elemento de comunicação entre o CD do IST ou CIIST e o Departamento/Grupo de Investigação, sempre que tal seja necessária.
  - Estabelecer um modelo de funcionamento das máquinas e da sub-rede local que permita a existência de uma assistência técnica continuada.
  - Criar as condições necessárias para a implementação de políticas que venham a ser definidas centralmente pelo IST e que sejam consideradas indispensáveis para a segurança ou bom funcionamento da rede do IST.
  - Nomear a equipa técnica e o responsável técnico pela pela gestão e manutenção da sub-rede local e das máquinas associadas.
  - Comunicar ao CIIST o nome e contactos do responsável técnico e dos outros elementos da equipa de manutenção da sub-rede e das máquinas envolvidas.
- (N) O nome e contacto do responsável administrativo deverá ser comunicado ao CIIST pela estrutura competente do Departamento ou centro de investigação.
- (S) Cada Departamento, Grupo ou Instituto de Investigação deverá nomear apenas um responsável pela generalidade da rede e máquinas que lhe estão afectas, embora não se exclua a possibilidade de existirem mais do que um responsável em casos em que a estrutura interna ou divisão em unidades orgânicas assim o aconselhe.

2.3 Responsabilidade técnica

- (N) Todas as máquina ou sub-rede do IST devem ter um responsável técnico directo, o qual assumirá a responsabilidade pela manutenção das máquinas ou sub-redes e a intervenção directa sempre que necessário.

O responsável técnico poderá ser qualquer pessoa, interna ou externa ao IST, mas com os conhecimentos mínimos indispensáveis sobre a sub-rede e as máquinas pelas quais é responsável para poder ser interlocutor do CIIST sempre que tal seja necessário.

- (N) Caso o responsável técnico seja externo ao IST, deverá ter as autorizações necessárias de acesso para poder intervir junto das máquinas sempre que tal seja necessário.
- (R) Ao responsável técnico, competirá:
  - Garantir a manutenção e segurança das máquinas pela quais é responsável.
  - Garantir que as configurações adoptadas são seguras e não perturbadoras da rede do IST.
  - Manter-se a par de avisos de segurança emitidos pelo CERT, realizando todas as actualizações que sejam críticas numa perspectiva de segurança da rede do IST.
  - Subscrever a lista de e-mail IST-Sysadm, mantendo-se a par das principais informações referentes ao funcionamento do *backbone* de rede do IST.
- (S) Além do responsável técnico, deverá existir um ou mais elementos técnicos alternativos com os conhecimentos indispensáveis para identificar as máquinas por IP e capazes de intervir ou desligar as máquinas quando o responsável técnico não esteja disponível

2.4 Registo de responsáveis

- (N) É obrigatório o registo dos responsáveis técnicos e administrativos junto do CIIST.

Espera-se vir a disponibilizar um sistema de registo e consulta automatizado de IPs dos responsáveis técnicos e administrativos pelas várias redes do IST.

Até que este sistema esteja disponível, o registo dos responsáveis deverá ser realizado por e-mail enviado para ci@ist.utl.pt.

Capítulo 3

Normas Técnicas

3.1 Introdução

Descrevem-se neste capítulos as normas técnicas em vigor na rede do IST e que deverão ser consideradas na administração de sub-redes e máquinas de redes e departamentos do IST.

3.2 Segurança

3.2.1 Responsabilidade

A segurança é uma preocupação fundamental na gestão de redes informáticas. Os responsáveis técnicos pelas sub-redes e máquinas de Centros e Departamentos deverão assumir a responsabilidade pelas falhas de segurança das máquinas que lhes estão afectas.

Na administração de sub-redes do IST deverá ser considerada, com particular preocupação, a responsabilidade civil que possa vir a ser atribuída ao IST em virtude de violações de segurança, ou outros crimes de natureza informática que tenham origem na rede do IST. Sendo certo que, em alguns casos, tais situações são difíceis de controlar totalmente, deverão ser tomadas todas as medidas possíveis para que tais situações sejam evitadas ou minimizadas.

Para além de eventuais problemas de natureza legal, convirá ter-se presente que a comunidade utilizadora da Internet usa hoje em dia vários mecanismos de controlo informal, frequentemente tão ou mais eficazes nos danos produzidos à imagem e funcionalidades das instituições que o re-

curso a mecanismos legais. Um dos sistemas mais frequentes é a manutenção de *listas negras* (*black lists*) de máquinas (ou mesmo de sub-redes inteiras) que já foram identificadas como base para a realização de acessos ilegais, distribuição de mail não solicitado ou outras acções que coloquem em risco a segurança e eficiência da rede pública. Nestes casos, o resultado de um erro de administração ou de uma vulnerabilidade não corrigida pode levar à colocação das máquinas ou redes responsáveis numa lista negra, com sérios prejuízos para a comunidade de utilizadores dessa rede (nomeadamente, rejeição total do mail enviado ou bloqueio do acesso a determinadas *sites*).

- (I) Caso sejam detectadas situações de ataques a ou acções ilegais a partir da rede do IST que possam ter tido origem em vulnerabilidades resultantes de negligência óbvia por parte do responsável técnico, o CIIST reportará a situação ao responsável administrativo e ao Conselho Directivo do IST, de modo a serem tomadas medidas adequadas.

3.2.2 Segurança física

- (R) Os responsáveis administrativos e técnicos deverão estabelecer as medidas necessárias para que exista alguma forma de controlo no acesso físico às máquinas.
- (R) Em caso de salas de alunos, deverá haver formas de controlo que impeçam a utilização livre do equipamento por elementos estranhos ao Instituto Superior Técnico.

3.2.3 Actualizações de segurança

O responsável técnico deverá:

- (R) Estar atento aos avisos de segurança emitidos directamente pelo CERT, divulgados pelo serviços cert.pt ou anunciados na lista de mail ist-sysadm.
- (N) Garantir que todas as máquinas sob a sua responsabilidade directa têm aplicadas as revisões de software (*patchs* e *upgrades*) que sejam anunciadas e publicadas e que estejam relacionadas com vulnerabilidades identificadas de serviços e sistemas operativos.

3.2.4 Anti-vírus

- (N) Todas as máquinas com sistema operativo Windows ligadas à rede do IST deverão estar convenientemente protegidas por aplicações de *anti-vírus* apropriadas.

Chama-se a atenção de que o IST dispõe de licenças de campus para produtos anti-vírus que abrangem todas as máquinas ligadas à rede do IST, incluindo as que são propriedade de alunos, docentes ou funcionários. Para mais informações, consultar http://delta.ist.utl.pt/ e http://avalis.ist.utl.pt/.

3.2.5 Acessos do exterior

- (N) Todos os acessos a partir do exterior a contas privadas deverão ser protegidos por um sistema de segurança adequado (*username/password*, certificados ou outro), capazes de identificar de forma inequívoca o utilizador do acesso.
- (R) No caso do acesso ser realizado por *username/password* deverão ser totalmente eliminados os protocolos ou serviços em que a *password* circule em claro. Incluem-se, entre outros:
  - *rlogin*
  - *telnet*
  - *ftp*
  - *pop3*
  - *imap*
  - Autenticação por *http*

  Caso algum destes protocolos seja necessário, o mesmo deverá ser substituído por uma versão segura equivalente (baseada em criptografia assimétrica ou outra) ou só ser disponibilizado através de túneis seguros (SSL ou VPN).
- (S) Exceptua-se da norma anterior situações específicas em que um destes protocolos seja necessário para dar acesso a uma única conta de acesso público. Nestes casos, a conta pública deverá ter o acesso limitado e as suas permissões restringidas aos fins a que se destina, não podendo em caso algum servir de *relay* para acessos à rede interna do IST. Em particular, é estritamente proibida a instalação de *proxys* de acesso público em qualquer máquina do domínio do IST.

3.2.6 Monitorização da rede

Devido à possível exploração de falhas ou abuso de utilização do protocolo ICMP, durante algum tempo generalizou-se a ideia de que o protocolo ICMP deveria ser bloqueado em todos as

máquinas, com especial incidência em *routers* e *firewalls*. Esta prática popularizou-se também depois de alguns ataques de *Denial Of Servcice* baseado em pacotes ICMP.

No entanto, o protocolo ICMP é uma componente fundamental do protocolo IP e, como é bem conhecido, uma ferramenta de monitorização fundamental para aferir o bom funcionamento da rede, sendo por vezes extremamente difícil aferir o bom funcionamento de uma rede sem a sua contribuição.

Deste modo, deverão ser tidos em conta os seguintes princípios na gestão de *routers* e *firewalls*:

- (N) Todos os *routers* e *firewalls* do IST deverão responder obrigatoriamente aos seguintes pacotes ICMP:
  - ICMP destination unreachable - fragmentation needed but DF bit set;
  - ICMP time exceeded;
  - ICMP echo request e ICMP echo reply.
- (R) Caso se verifique a necessidade de limitar o tráfego ICMP, tal deverá ser feito preferencialmente colocando limites ao volume de tráfego ICMP e não pelo seu bloqueio incondicional.

3.3 Gestão do Espaço de Endereçamento

3.3.1 Atribuição de IPs

A fracção do espaço de endereçamento atribuído pela UTL ao IST é gerida e administrada pelo CIIST. Este espaço de endereçamento encontra-se distribuído pelos diversos edifícios, serviços e entidades existente nos dois pólos do IST.

Por motivos de operacionalidade de gestão, a administração dos endereços de alguma sub-redes encontra-se delegada numa única entidade do IST. Em alguns caso, esta delegação encontra-se associada à delegação do serviço de nomes (DNS) de um determinado sub-domínio do domínio *ist.utl.pt*,

Na administração de endereços IP, deverá ter-se presente as seguintes normas:

- (R) Por razões de segurança, deverá ser evitada a utilização de IPs públicos em computadores de utilização pessoal, excepto se os mesmos estiverem instalados numa subrede e isolados do *backbone* de rede por um *gateway/router* munido de uma *firewall* conveniente.

  Alternativamente, as máquinas poderão ser ligadas à rede do IST por meio de uma NAT box com único IP público e utilizar endereços privados.

  Pelo menos um dois mecanismos de protecção anteriores deverá obrigatoriamente ser adoptado em máquinas de LTIs ou de utilização colectiva, em que a grande rotatividade de utilizadores coloca dificuldades acrescidas na responsabilização individual dos utilizadores e na garantia da segurança lógica dos equipamentos.

- (N) A utilização de IPs públicos do IST deverá ser sempre solicitada ao CIIST.

  Exceptuam-se desta norma situações em que tenha havido uma delegação da administração de um sub-domínio do domínio ist.utl.pt conjuntamente com uma gama específica de IPs (situação que será abordada na secção 3.4).

- (N) Todos os IPs públicos em utilização no IST deverão obrigatoriamente estar declarados e acessíveis por nome num servidor de nomes (DNS). Deste modo, é estritamente proibida a utilização de IPs públicos não registados num serviço de DNS do IST.

  Exceptuam-se apenas desta norma os casos particulares, devidamente fundamentados, em que tal registo seja eventualmente desaconselhado por razões de segurança.

- (I) O pedido de utilização de um IP público deverá ser feito por mail enviado ao CIIST para ci@ist.utl.pt indicando o nome que deverá ser associado no serviço de DNS.

- (R) Todos os IPs públicos em utilização do IST deverão ter uma referência no mapa inverso correspondente.

- (I) O CIIST reserva-se o direito de bloquear o acesso ao exterior ou a serviços internos do IST a qualquer IP público do IST que não esteja devidamente registado no CIIST ou cujo nome não surja no mapeamento inverso.

- (R) Todos os endereços públicos IP do IST deverão estar registados numa base de dados de IPs que incluirá os nomes e contactos dos responsáveis técnicos e administrativos.

- (N) Os responsáveis técnicos e administrativos deverão manter registos actualizados dos IPs de todas as máquinas que estejam sob a sua administração directa, incluindo a localização da máquina e/ou a identificação do responsável directo pela mesma.

- (I) Mesmo em situações em que a totalidade dos endereços de uma dada sub-rede pública do IST tenha sido delegada numa única entidade ou responsável, deverá ter-se presente que a responsabilidade da gestão IPs públicos do IST é, em última análise, do CIIST. Assim, caso se verifique erros graves na utilização ou administração de endereços, esta delegação poderá ser retirada.

3.3.2 NAT boxes

Tal como referido anteriormente, a utilização de NAT boxes é uma das soluções de segurança aconselháveis para o isolamento lógico a grupos de máquinas de utilização pessoal e em que o endereço público não seja estritamente indispensável.

- (N) Sempre que um dado IP seja utilizado para uma NAT box, o responsável técnico deverá informar o CIIST deste facto.
- (R) Esta informação deverá mantida actualizada na base de dados central de IPs, incluindo uma estimativa actualizada do número de máquinas que partilham o endereço público.

O registo de NAT boxes é obrigatório por duas razões fundamentais:

- Por motivos técnicos e administrativos, o CIIST tem que conhecer com uma boa precisão o número de máquinas ligadas à infra-estrutura de rede do IST. Isto só é possível conhecendo o n**?** aproximado de máquinas existentes atrás de cada NAT box.
- O CIIST limita o número de máximo de ligações que pode ser estabelecido por um mesmo IP, dado que um número excessivo destas ligações indicia geralmente uma utilização abusiva da rede. Como é evidente, no caso de NAT boxes, o número de ligações a autorizar deverá ser significativamente aumentado.

3.3.3 Servidores de DHCP

A utilização de servidores de DHCP é uma forma comum de automatizar a distribuição de endereços IP. Na instalação de servidores de DHCP deverão ser seguidas as seguintes normas:

- (N) Por razões técnicas óbvias, é interdita a ligação de servidores de DHCP ao *backbone* de rede do IST ou em segmentos de rede que não estejam devidamente isolados e identificados.
- (R) Como decorre das normas da secção 3.3.1, a distribuição de IPs públicos por meio de servidores de DHCP deve ser evitada e, a realizar, carece de autorização prévia do CIIST.
- (R) A eventual distribuição de IPs públicos por DHCP não invalida a obrigatoriedade de todos os IPs distribuídos ou disponíveis para distribuição estarem convenientemente registados em servidores de DNS bem como nos mapas inversos correspondentes.

- (R) Sempre que possível, a distribuição de IPs por DHCP (públicos ou não) deve ser for acompanhada por medidas complementares de segurança (registo de endereços MAC, protocolo 802.1X, sistema de VPN ou outro) que permita a identificação inequívoca do utilizador.
- (R) A norma referida no parágrafo anterior deverá ter carácter obrigatório no caso de distribuição por DHCP de IPs públicos.

3.3.4 Gestão de endereços privados

- (N) Sempre que forem instaladas redes privadas com ligação por meio de NAT boxes, os endereços privados adoptados deverão obrigatoriamente ser os previstos no RFC 1918 do IETF:

Gama de endereços	rede/máscara	N. de endereços
10.0.0.0 - 10.255.255.255	10.0.0.0/8	16,777,216
172.16.0.0 - 172.31.255.255	172.16.0.0/12	1,048,576
192.168.0.0 - 192.168.255.255	192.168.0.0/16	65,536

No IST nunca foi definida uma política coordenada de utilização de endereços privados. Deste modo, a instalação de NAT boxes e a utilização de endereços privados tem sido realizado de forma autónoma por Departamentos, Centros e Grupos de Investigação, os quais têm escolhido de forma *ad-hoc* os endereços privados utilizados. Deste modo, é provável a duplicação e conflitos de endereços privados. Embora esta situação não seja em si grave, impede o estabelecimento uma política global de encaminhamento consistente de endereços privados, ou seja, não é possível, por exemplo, realizar um encaminhamento selectivo de endereços privados de duas sub-redes que pretendam comunicar entre si. Por outro lado, o próprio CIIST tem utilizado tradicionalmente endereços de gamas privadas para a gestão de equipamento de rede, definindo as políticas de encaminhamento tendo apenas em consideração os endereços utilizados directamente pelos seus serviços técnicos.

Deste modo, na utilização de endereços privados, deverão ser consideradas os seguintes pontos:

- (I) De uma forma geral, não existe uma forma consistente de definir encaminhamento de endereços privados entre as sub-redes privadas do IST.
- (N) É proibido o encaminhamento de endereços privados de sub-redes de Grupos e Departamentos para a rede geral do IST, com excepção dos utilizados directamente pelo CIIST para administração e gestão da rede.

- (I) Em casos pontuais em que seja conveniente o encaminhamento de endereços privados entre sub-redes de Departamentos, Grupos ou Instituições na rede geral do IST, tal facto deverá ser comunicado ao CIIST, com indicação do encaminhamento pretendido.

  Caberá ao corpo técnico do CIIST avaliar a sua exequibilidade e compatibilidade com os endereços já em utilização.

- (I) Não se exclui a possibilidade de, no futuro, o CIIST vir a estabelecer uma política geral de distribuição interna de IPs privados, o que poderá aconselhar a revisão das gamas de endereços privados em utilização.

3.4 Serviço de DNS e delegação de domínios

3.4.1 Introdução

Em algumas situações, a gestão de nomes de determinados Departamentos e Institutos de Investigação foi delegada nos próprios serviços técnicos dessas entidades. Em certos casos, esta delegação de nomes foi acompanhada da delegação da gestão de uma dada sub-rede de IPs.

Apesar desta delegação de domínios, deverá manter-se presente que os técnicos dos serviços centrais da UTL e do IST são os registados no RIPE e a quem, em última instância, cabe a responsabilidade técnica pela correcta gestão dos IPs atribuídos ao IST. Deste modo, deverá manter-se presente que:

- (I) A delegação de domínios pressupõe uma elevada responsabilização técnica por parte dos serviços técnicos das entidades em que tal gestão seja confiada.

- (I) A delegação pressupõe a existência de um corpo técnico facilmente contactável, e actualizado, que possa cooperar com o CIIST na resolução de problemas que afectem a gestão de IPs desses domínios (ou outros serviços delegados, como a gestão de servidores de mail, que será abordada na secção 3.5).

- (R) A delegação de domínios implica a aceitação e observância por parte das entidades em que a delegação é realizada das normas gerais em vigor no IST.

- (I) A delegação de um dado domínio poderá ser retirada pelo CIIST caso se verifique erros graves na administração dos mesmos ou em caso se verifique a impossibilidade dos responsáveis de manter a sua gestão dento dos parâmetros de segurança e de qualidade definidos globalmente para a escola.

3.4.2 Gestão de DNS

A delegação da gestão do serviço de nomes (DNS) a sub-domínios implica que o responsável técnica cumpra os princípios gerais em vigor no IST para a a gestão de IPs públicos enunciados anteriormente:

- (N) Todos os IPs públicos em utilização no IST deverão obrigatoriamente estar declarados e acessíveis por nome num servidor de nomes (DNS).
- (N) Nos casos em que uma delegação de domínio tenha sido acompanhada pela delegação da gestão de uma gama de IPs, o servidor de DNS deverá manter actualizados os mapas inversos da rede correspondente.
- (N) É estritamente proibida a utilização de IPs públicos não registados num serviço de DNS do IST.
- (R) A utilização de IPs públicos em domínios delegados não dispensa o seu registo na base de dados de IPs públicos do IST, assim que esta esteja disponível
- (R) Os domínios delegados deverão observar as mesmas normas enunciadas na secção 3.3.3 relativas à distribuição por DHCP de IPs públicos.

3.4.3 Registos obrigatórios

- (N) Todos os domínios delegados deverão ter um registo MX correspondente a um servidor de mail válido do domínio ist.utl.pt.

Sugere-se fortemente a utilização como MX primários um dos servidores primários do CIIST com serviço de *anti-spam* e *anti-vírus* (consultar http://ciist.ist.utl.pt/servicos/mail/avirus.php).

3.4.4 Servidores secundários

- (N) Em caso de delegação de domínios, a entidade responsável pelo domínio delegado deverá garantir a manutenção de, pelo menos, um servidor secundário.
- (R) O servidor secundário obrigatório deverá ser mantido numa máquina exterior à própria entidade.
- (S) Preferencialmente, o servidor secundário deverá estar localizado fora do IST.

3.4.5 Domínios com nomes alternativos a .ist.utl.pt

Surge por vezes a conveniência ou necessidade de registar domínios com nomes alternativos aos possíveis no domínio **.ist.utl.pt**, como por exemplo *www.conference.org* ou similares.

As normas a seguir nestes casos são explicitdas na secção 4.4 deste documento.

3.5 Gestão de mail

3.5.1 Introdução

Nos últimos anos, o mail tornou-se o principal mecanismo de propagação de *vírus* e *worms*. Adicionando a este facto a proliferação de mail não solicitado (*spam*), uma gestão eficaz de servidores de mail é hoje essencial para garantir a qualidade de serviço prestado, manter a segurança interna da rede e limitar o risco de utilização da rede do IST como base para a distribuição ilegal de mail (spam).

3.5.2 Instalação de servidores de SMTP

O CIIST tem disponível um sistema robusto e fiável de mail no domínio ist.utl.pt, o qual pretende continuar a desenvolver de modo a aumentar o seu nível de redundância, capacidade de armazenamento e serviços disponíveis. Os servidores de SMTP do CIIST estão dotados de sistemas de anti-vírus e marcação de *spam*, além de terem disponíveis para consulta de mail de servidores de *webmail* e protocolo *pop3s*.

- (S) Dada a importância que assume actualmente todo o sistema de mail e a necessidade de uma gestão profissional e permanente dos seus servidores, o CIIST desencoraja actualmente a instalação de servidores de SMTP próprios por parte das entidades que utilizam a rede do IST. O CIIST sugere, alternativamente, a utilização dos servidores centrais da escola para este efeito.

  Note-se que, para as entidades e utilizadores que o pretendam, é possível gerar aliases alternativos de mail (por exemplo, *destinatario@entidade.ist.utl.pt*), pelo que a utilização de endereços de mail alternativos não deve ser considerado impeditivo da utilização dos servidores de mail central.

- (I) Caso a instalação de um servidor SMTP tenha por único objectivo a gestão de listas de mail, recorda-se que CIIST dispõe de um serviço de administração de listas de *mail* em http://mlists.ist.utl.pt.

De qualquer modo, dada a sensibilidade dos servidores de mail, a autorização para instalação de novos servidores no IST está condicionada à observância das normas estabelecidas no seguimento.

3.5.3 Registo de servidores de SMTP

- (I) Dada a proliferação de vírus que instalam servidores *ad-hoc* de SMTP, todos os acessos pela porta 25 encontram-se bloqueados na *firewall* do IST, com excepção de servidores explicitamente autorizados pelo CIIST.
- (N) Como consequência do ponto anterior, todos os servidores SMTP do IST deverão obrigatoriamente ser registados no CIIST.

  O CIIST reserva-se o direito de não autorizar este registo ou cancelar o acesso ao exterior caso se verifique que o servidor não verifica as normas de segurança e de funcionamento definidas neste documento.

3.5.4 Política anti-spam

Política anti-spam da RCTS

O acesso da rede do IST/UTL à Internet é realizado por intermédio da Rede Ciência, Tecnologia e Sociedade (RCTS), gerida pela FCCN. Foi já definida por parte desta entidade uma política de anti-spam, disponível nas páginas da FCCN.

Por inerência, o IST está já obrigado a seguir a política anti-spam da RCTS. Nesta secção, regulamenta-se apenas alguns aspectos particulares desta política.

Envio de mail não solicitado

- (N) É estritamente interdita a utilização da rede do IST para o envio de mail não solicitado anónimo ou de natureza comercial.

- (R) De uma forma geral, considera-se abrangido pela norma do ponto anterior e pela noção de *mail não solicitado* a utilização extensiva e indiferenciada de endereços do IST para a divulgação de opiniões pessoais ou outras, mesmo quando o mail seja assinado e tenha origem num endereço de mail do próprio IST.

  Não estão abrangidos por esta norma os avisos enviados por entidades competentes ou mails enviados para listas de mail específicas para a discussão de tópicos, divulgação de informações ou outros temas que estejam claramente abrangidos pelo âmbito da lista de mail utilizada.

- (R) Todos os mails enviados para o exterior do IST para a divulgação de eventos ou outros anúncios que não sejam exclusivamente destinados a listas especializadas ou moderadas deverão ser tanto quanto possível evitados.

- (N) Em casos pontuais em que o autor considere adequada a utilização do envio de anúncios ou avisos de divulgação para colecções de endereços de mail, de elevada dimensão, coligidos individualmente (por exemplo, listas de participantes em eventos passados, relacionados ou outras), deverão ser tomados em atenção os seguintes pontos:

  - (S) Deverá existir firme convicção de que o destinatário se encontra interessado ou que aceitará a divulgação da informação prestada por esta estar relacionada com um tópico do seu interesse.
  - (N) Os destinatários da mensagem deverão estar mutuamente ocultos.
  - (R) A divulgação deverá ser realizada criando uma lista de mail com um endereço de mail único e um nome claramente sugestivo do âmbito e abrangência do tópico criado.
  - (N) Todos os mails enviados desta forma deverão incluir, obrigatoriamente:
    * A identificação clara do responsável pelo evento ou informação de origem.
    * O endereço de email do responsável pelo mail ou um endereço de mail específico da entidade, organização ou evento que possa ser utilizado para contacto do responsável.
    * Informação clara sobre a forma como o destinário pode eliminar o seu nome da lista de mail criada (*unsubscribe*). Este sistema de eliminação deverá ser automatizado.
    * O mail deverá incluir, no final, a seguinte indicação ou equivalente:
      Esta mensagem está de acordo com a legislação Europeia sobre o envio de mensagens comerciais: qualquer mensagem deverá estar claramente identificada com os dados do emissor e deverá proporcionar ao receptor a hipótese de ser removido da lista. Para ser removido da nossa lista, basta que nos responda a esta mensagem colocando a palavra **Remover** *no assunto. (Directiva 2000/31/CE do Parlamento Europeu; Relatório A5-270/2001 do Parlamento Europeu).*

Este texto deverá ser traduzido no caso de divulgação internacional e deverá ser adaptado no que se refere à forma específica de remoção automática suportada.

Relaying de mail

- (N) É estritamente proibida a configuração de servidores que façam encaminhamento aberto (*open relay*) de mail. Assim, não é autorizada o *relay* de mail que não tenha origem ou destino no domínio *.ist.utl.pt*
- (S) Desejavelmente, um dado servidor de mail só deverá fazer *relay* do sub-domínio a que se encontra associado.

Mapas inversos

- (S) Todos os servidores de SMTP deverão estar declarar no mapa inverso de DNS correspondente (a obrigatoriedade deste mapeamento decorre também das normas enunciadas na secção 3.3.1).
- (S) Actualmente, existem vários servidores de mail que recusam o *relaying* de mail proveniente de servidores sem mapeamento inverso como forma de minimizar a distribuição de *spam*.

  Apesar de se considerar este princípio razoável, a experiência do CIIST (Dez. 2004) aponta para que existe ainda um elevado número de servidores lícitos de mail cujos nomes ainda não surgem correctamente no mapeamento inverso, em Portugal e no estrangeiro. Deste modo, considera-se desaconselhável e demasiado restritiva adoptar esta configuração em servidores de mail do IST.

Serviço de anti-spam

- (R) Todos os servidores SMTP do IST deverão ter um serviço de identificação e marcação de mails com *spam*.
- (S) Deverá existir um mecanismo que permita a um utilizador individual prescindir do serviço de marcação de *spam*

3.5.5 Servidores de *pop3*, *imap* e *webmail*

- (R) Como já referido na secção 3.2.5, os serviços de *pop3* e *imap* implicam a transmissão da *password* em claro, pelo que deverão ser evitados.
- (R) Sempre que necessários, os protocolos *pop*3 e *imap* deverão ser substituídas pelas versões equivalentes baseados em criptografia assimétrica (*pop3s* e *imaps*).
- (S) Embora a utilização dos protocolo *pop*3 e *imap* no âmbito de uma rede privada possa ser aceitável, sugere-se vivamente a eliminação progressiva destes protocolos e a sua substituição pelas versões seguras.
- (N) Em caso de disponibilização de um serviço de *webmail* este deve obrigatoriamente ser disponibilizado apenas sobre o protocolo *https* (disponibilizando, eventualmente, um redireccionamento automático a partir de um primeiro acesso *http*).
- (I) Para obter certificados assinados pelo IST, consultar http://ra.ist.utl.pt.

3.5.6 Serviço de anti-vírus

- (R) Todos os servidores SMTP do IST deverão ter um serviço de identificação e filtragem de mails com vírus.
- (R) O serviço de anti-vírus deverá filtrar mails recebidos e evitar a expedição de mails com vírus a partir da rede do IST.
- (R) Na recepção, as componentes com vírus do mail deverão ser eliminadas, devendo ser adicionado um texto ao corpo da mensagem avisando o destinatário deste facto.
- (R) Caso sejam identificados vírus numa mensagem expedida a partir do IST, o envio da mensagem deve ser cancelado, devendo o emissor ser avisado deste facto.
- (S) Sugere-se a utilização dos servidores de anti-vírus e de anti-spam do CIIST para este efeito.

3.5.7 Filtragem de anexos

- (S) De modo a evitar a propagação de vírus na rede do IST, sugere-se vivamente a eliminação preventiva de anexos com ficheiros executáveis dos tipos normalmente utilizados para propagação de vírus e que raramente são utilizados como anexos lícitos pelos utilizadores

Para uma lista completa dos anexos normalmente filtrados pelos serviços do CIIST, consultar http://ciist.ist.utl.pt/servicos/attach.php

3.6 Redes sem fios

A norma 802.11 utiliza 13 canais na banda do 2.4Ghz, mas, infelizmente, apenas 3 destes canais são disjuntos e podem ser utilizados simultaneamente. A planificação da cobertura total do IST pela rede central (WiFi_IST) exige a utilização de todos estes canais de modo à não interferência entre pontos de acesso próximos, cujas zonas de cobertura se intersectem parcialmente. Adicionalmente, dado que a tecnologia de redes sem fios configura uma forma simples de acesso à rede do IST, cuja segurança é centralmente da responsabilidade do CIIST, o acesso à rede só deverá ser possível mediante a adopção dos mecanismos de segurança estabelecidos centralmente.

Deste modo, qualquer utilização de outras redes na área do IST colide com pontos de acesso já existentes com a rede geral do IST, cujo planeamento e cobertura pode ser seriamente afectado. Por este motivo,

- (N) A instalação de redes privadas sem fios é actualmente estritamente interdita dentro do recinto do IST.
- (I) Exceptua-se da norma anterior utilização da tecnologia sem fios para investigação em áreas em que o recurso a esta tecnologia seja indispensável ou o próprio objecto de investigação.

  Incluem-se nestes casos a investigação em redes sem fios, aplicações de robótica móvel e outra em que esta tecnologia seja indispensável. Em qualquer dos casos, os utilizadores destas tecnologias deverão entrar em contacto com o CIIST de modo a serem definidas soluções que minimizem o impacto na rede central do IST.

  Nestes casos, as redes envolvidas e acessos permitidos deverão ser isolados da rede geral do IST.

Capítulo 4

Políticas de utilização da rede do IST

4.1 Regras de acesso à RCTS

A FCCN publicou uma carta ao utilizador. que enuncia princípios gerais e restrições para a utilização da RCTS.

Sem prejuízo de outras disposições da RCTS, que deverão sempre ser respeitadas, destacam-se os seguinte princípios gerais:

- (N) A utilização da RCTS deverá ser coerente com o objectivo principal da própria rede: servir a comunidade de ensino, investigação e cultura.
- (N) A utilização da RCTS não se destina a fins comerciais, nomeadamente fins publicitários. Constitui excepção a esta regra a divulgação de actividades próprias das Entidades Utilizadoras (EU), nomeadamente das publicações por elas editadas e dos cursos que ministrem.
- (N) Não é permitida a uma EU, com uma Porta de Acesso à RCTS, facultar o acesso a outra pessoa, singular ou colectiva, sem autorização prévia da FCCN.

Esta secção, regulamenta-se apenas alguns aspectos particulares desta política no IST, sem prejuízo de outros princípios já definidos no documento Uso Aceitável dos Recursos Informáticos no IST.

4.2 Utilização da rede do IST

Na sequência das normas gerais da RCTS, destacam-se os seguintes princípios essenciais constantes no documento Uso Aceitável dos Recursos Informáticos no IST:

- (N) Nenhum sistema informático do IST pode ser usado para finalidades não éticas ou ilegais por natureza, ou que violem o espírito de leis locais ou internacionais.
- (N) Nenhum sistema informático do IST pode ser usado para finalidades não académicas ou que entrem em conflito com a missão ou políticas do IST, tais como a promoção de causas de política partidária ou a transferência ou armazenamento de material que contenha referências obscenas ou pornográficas.
- (N) Nenhum sistema informático do IST pode ser usado para fins comerciais, incluindo a condução de uma empresa pessoal usando recursos do IST ou o nome ou a reputação do IST. Tais usos proibidos abrangem, mas não são limitados a, desenvolvimento de programas, processamento de dados ou preparação e apresentação de material publicitário.

4.3 Normas de utilização de recursos informáticos do IST

Os recursos informáticos são frequentemente utilizados para troca de mails, definição de listas de mail, alojamento de páginas e a instalação de fóruns de discussão.

Na utilização de recursos informáticos do IST deverão ser tomadas em consideração as seguintes disposições gerais:

- (N) Os recursos informáticos do IST deverão prioritariamente ser destinadas a fins académicos e científicos.
- (I) Considera-se aceitável a utilização de recursos do IST para fins culturais, desportivos ou sociais, de natureza não comercial, desde que essa utilização seja autorizada pelo responsável máximo do Grupo, Departamento ou Centro de Investigação em que o servidor seja instalado e que essa utilização não colida com os princípios gerais definidos nas regras da RCTS e do Uso Aceitável definido no IST.
- (S) Em caso de dúvida sobre a legalidade de concessões específicas referidas no item anterior, deverá ser contactado o CIIST, o qual, consoante as circunstâncias, poderá emitir um parecer ou submeter o caso ao Conselho Directivo do IST.

- (I) As autorizações de utilização para fins específicos dispostas no item anterior poderão ser canceladas superiormente pelo Conselho Directivo do IST se se verificar que essa utilização contraria as normas gerais em vigor, coloca em causa o desempenho da rede ou que essa utilização possa colidir com a utilização da rede para os fins primários a que se destina.

4.4 Registo de domínios com nomes alternativos

No âmbito das suas actividades, é frequente as entidades que utilizam a rede do IST registarem domínios com nomes específicos, externos ao domínio **.ist.utl.pt**, são associados a endereços IP do IST (por exemplo, *www.conference.org* ou similares).

No registo de nomes alternativos associados a endereços do IST, deverão ser tomados em consideração as seguintes normas:

- (N) O registo de nomes alternativos redireccionados para servidores instalados na rede do IST deverá ser sempre objecto de informação ao CIIST, por intermédio de mail enviado para *ci@ist.utl.pt*.
- (I) Os domínios alternativos deverão estar associados a eventos reconhecidos no âmbito científico ou académico.
- (I) Em caso de utilização de nomes alternativos para outros fins, deverão ser tomadas consideração as restrições enunciadas na secção 4.3.
- (N) Em caso de utilização de domínios alternativos para actividades de índole social, cultural ou desportiva como as referidas na secção 4.3, a página principal de acesso deverá conter pelo menos uma referência explicitando que o servidor se encontra alojado numa máquina do IST.

4.5 Violação de direitos de autor

Desde há alguns anos, a Internet é utilizada de forma intensiva para a violação de direitos de autor. Na maioria dos casos, esta utilização ilícita da rede tem lugar pela partilha ilícita de ficheiros, usando programas que utilizam protocolos *peer-to-peer* (vulgo p2p).

Dado que a utilização destes protocolos e de cópias legais dos programas que usam estes protocolos não é em si ilícita, o CIIST não proíbe a sua utilização. No entanto, a utilização destes

programas para a cópia de material com direitos de autor pode constituir um acto ilícito e, como tal, não autorizado pelas normas da RCTS e do IST. Para mais informação sobre a legislação existente sobre direitos de autor, consultar a página https://ciist.ist.utl.pt/normas/index.php.

Dada a frequência com que têm sido recebidas queixas de violação de direitos de autor nos serviços responsáveis do IST e da FCCN por parte de indivíduos, entidades e seus representantes legais, o IST definiu os seguintes procedimentos para abordagem deste problema:

- (N) Todos as queixas referentes a violação de direitos de autor recebidas formalmente pelo IST serão previamente avaliadas para aferir a autenticidade do remetente.
- (N) Caso a queixa recebida contenha uma assinatura electrónica que comprove a autenticidade do remetente, o CIIST adoptará as seguintes medidas:
  - (N) A queixa será registada internamente pelo CIIST.
  - (N) Caso o IP não corresponda a uma NAT box registada no CIIST (recorde-se que este registo é obrigatório, como referido na secção 3.3.2), o acesso ao exterior deste IP será imediatamente cortado, e a informação correspondente será passada ao administrador da sub-rede em que o IP se encontra (nota: a suspensão do acesso ao exterior poderá ser adiado caso tal seja tecnicamente aconselhável para investigação e identificação do utilizador do IP referido na queixa).

    O acesso ao exterior será reposto assim que o administrador da sub-rede ou o próprio utilizador informe que cessou a utilização ilícita da rede ou que a denúncia era falsa.
  - (N) Caso o IP corresponda a uma NAT box registada no CIIST, a queixa será passada ao Administrador da sub-rede correspondente. Neste caso, o administrador da sub-rede ou o próprio utilizador deverá informar o CIIST que cessou a utilização ilícita da rede ou que a denúncia era falsa. Caso não seja recebida uma resposta dentro do prazo de cinco dias úteis, será vedado o acesso ao exterior do IP da NAT box.
  - (N) Em todas as situações anteriores, caso seja identificado o responsável directo pela queixa recebida, deverão ser adoptadas as seguintes medidas:
    - (N) O utilizador deverá ser pessoalmente notificado da queixa recebida, da qual deverá ter conhecimento integral.
    - (N) O utilizador deverá ser notificado de que deverá remover todo o material ilícito das máquinas pelas quais é responsável e que estejam ligadas à rede do IST. A remoção do material ilícito deverá ter lugar obrigatoriamente caso a máquina seja propriedade do IST. Caso a máquina seja particular, o utilizador deverá remover ou suspender quaisquer serviços responsáveis pela distribuição do material protegido.

    - (N) A identificação do utilizador será registada pelo CIIST, para efeitos de arquivo e eventuais procedimentos de natureza legal pelos quais a escola possa vir a ter que responder.
    - (N) Em caso de reincidência na utilização indevida da rede, o CIIST proporá ao Conselho Directivo do IST a instauração de um processo disciplinar.

- (R) Em casos em que seja impossível ou manifestamente difícil identificar o utilizador responsável pela origem da queixa, os administradores de sub-redes, nat-boxes e firewalls deverão tomar as medidas necessárias para restringir o acesso ao exterior de portos não indispensáveis às actividades regulares desenvolvidas nessa sub-rede.

Capítulo 5

Validade e revisões

Mais do que uma simples imposição ou enunciado de regras imutáveis, pretende-se que este documento constitua uma base de discussão e uma referência para todos os envolvidos na gestão da rede informática do IST. Espera-se, deste modo, estabelecer um conjunto de normas que contribuam para uma melhor articulação de responsabilidades entre os diversos participantes na gestão da rede e uma maior qualidade global da rede do IST.

Como é evidente, um documento deste tipo é sempre datado e polarizado pelos problemas tecnológicos decorrentes da data em que foi produzido. Espera-se que este documento seja sujeito a revisões periódicas de forma a poder acompanhar a evoluções tecnológica e da própria estrutura organizativa do IST.

De um modo geral, a discussão deste documento deverá ter lugar no âmbito do Conselho de Peritos do CIIST e da lista de mail ist-sysadm. A manutenção e revisão deste documento é da responsabilidade do Conselho Directivo do CIIST, tendo em atenção as críticas, comentários e sugestões e que lhe sejam dirigidas.