I Pesquisa de Segurança da Rede Acadêmica Brasileira

Análise de Resultados

I Pesquisa de Segurança da Rede Acadêmica Brasileira

Análise de Resultados


Shift

Sumário

Siglas

CAIS	Centro de Atendimento de Incidentes de Segurança
CPD	Centro de Processamento de Dados
CSIRT	Computer Security Incident Response Team
IFES	Instituições Federais de Ensino Superior
NAT	Network Address Translation
RNP	Rede Nacional de Ensino e Pesquisa
TIC	Tecnologia da Informação e Comunicação

Sobre a RNP

Responsável pela introdução da Internet no Brasil, em 1992, a RNP opera a rede acadêmica nacional, a rede Ipê. Sua missão é promover o uso inovador de redes avançadas no país. Mantida pelos Ministérios da Ciência e Tecnologia, da Educação e da Cultura, atua no desenvolvimento e na prestação de serviços em três áreas: infraestrutura de redes de alto desempenho, aplicações avançadas e formação de recursos humanos em redes. A rede Ipê é uma infraestrutura de alto desempenho para colaboração e comunicação em educação e pesquisa que alcança os 26 estados da federação e o Distrito Federal. A RNP está conectada às redes acadêmicas latino-americana (RedCLARA), europeia (Géant) e norte-americana (Internet2), além de ter conexão própria à Internet mundial.

Sobre o CAIS

Criado em 1997, o CAIS atua na detecção, resolução e prevenção de incidentes de segurança na Rede Acadêmica Nacional (Rede Ipê). Em seu site (www.rnp.br/cais), disponibiliza uma série de informações para alertar os internautas sobre as ameaças da rede. Além disso, mantém um canal de contato com seus clientes através do endereço cais@cais.rnp.br para onde devem enviar relatos de incidentes de segurança relacionados à Rede Ipê. No campo internacional, o CAIS mantém relações com as principais organizações relacionadas ao setor de segurança na Internet. É filiado desde setembro de 2001 ao Forum of Incident Response and Security Teams (First) e, desde setembro de 2005, também é parceiro de pesquisa do APWG (Anti-Phishing Working Group).

Apresentação

O Centro de Atendimento de Incidentes de Segurança (CAIS) da Rede Nacional de Ensino e Pesquisa (RNP) apresenta, neste documento, os resultados da 1ª Pesquisa de Segurança da Rede Acadêmica Brasileira, realizada em outubro de 2009.

Esta pesquisa teve como público alvo as Instituições Federais de Ensino Superior (Ifes) no Brasil. Abordou temas como gestão da segurança, capacitação, infraestrutura de segurança, conformidade e outros assuntos relacionados com segurança da informação.

O objetivo desta pesquisa é traçar o cenário atual em segurança da informação nas Ifes e servir como insumo para o planejamento de ações em segurança do CAIS/RNP nos anos futuros.

Participaram desta pesquisa 45 Ifes, distribuídas em 40 cidades do Brasil e localizadas nas regiões Norte (15,6%), Nordeste (26,7%), Centro-Oeste (6,7%), Sudeste (37,8%) e Sul (13,3%).

Ifes/Estado	Estado
1	AC, AM, AP, CE, DF, ES, GO, MA, MS, PI, PR, RO, RR, SC, SE
2	BA, PA, PB, PE, RN, SP
4	RS
5	RJ
9	MG

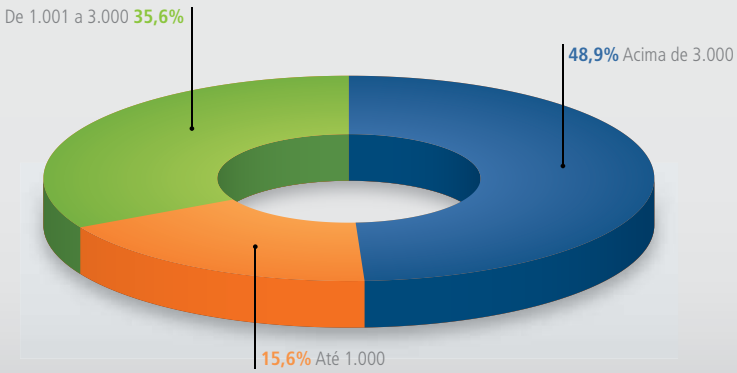
Metodologia

Os dados da pesquisa foram coletados através de um questionário on-line com 58 questões objetivas, sendo algumas de múltipla escolha. Responderam ao questionário 45 representantes da área de Tecnologia da Informação e Comunicação (TIC) das Ifes, correspondendo a 76,27% das Ifes brasileiras.

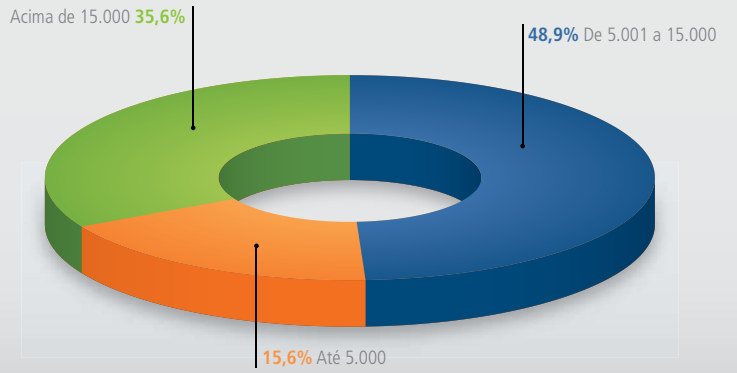
Perfil das Instituições

As Ifes são caracterizadas por possuírem redes com grande quantidade de usuários e estações de trabalho conectadas. Cerca de 48,9% das Ifes possuem mais de 3.000 computadores na rede de dados e 35,6% possuem mais de 15.000 usuários ativos.

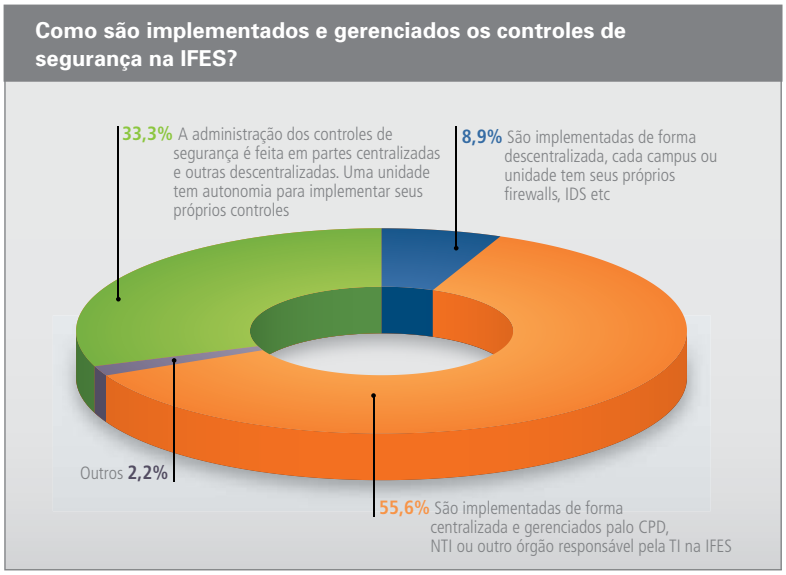
Qual a quantidade de estações de trabalho na IFES?



Qual a estimativa da quantidade de usuários ativos (alunos, professores, funcionários) da rede de computadores da IFES?



Em sua maioria (93,3%), as Ifes têm múltiplos campi, sendo que algumas instituições possuem campi em cidades distintas. Cerca de 55,6% das Ifes possuem a gerência de TIC centralizada no CPD, NTI ou órgão correspondente. Para 33,3% das instituições, a administração dos controles de segurança é feita em cada campus de forma indepedente. Ainda segundo a pesquisa, a gerência de TIC em diferentes campi é um dos principais desafios enfrentados, dada a dificuldade em implantar políticas centralizadas de TIC e segurança, sendo isto feito em 72,5% das instituições participantes.



Gestão da Segurança da Informação

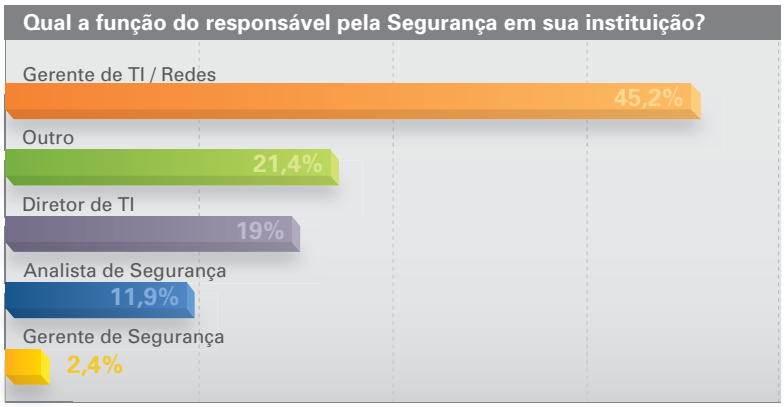
A principal deficiência identificada na pesquisa relaciona-se com a Gestão da Segurança da Informação, onde foram apresentados resultados com valores expressivamente negativos.

Estruturação da Segurança

A área de Segurança da Informação está estruturada em apenas 26,7% das Ifes. Para 73,3%, a segurança da informação consiste em atividades pontuais dentro da Gestão de TIC. Em 64,2% das instituições, o responsável pela Segurança da Informação é o Gerente de TI/Redes (45,2%) ou o Diretor de TI (19%), compartilhando assim as atividades de segurança com outras. O papel de Gerente de Segurança existe em apenas 2,4% das Ifes. Não existe o papel de CSO em nenhuma instituição participante da pesquisa.

Pouco mais da metade (54,8%) das Ifes que participaram da pesquisa afirmam ter uma carência de funcionários dedicados à segurança da informação. As demais instituições (45,2%) possuem de 1 a 3 funcionários focados nas atividades de segurança. O principal motivo é a falta de pessoal, um quadro presente na maioria das Ifes brasileiras.

Os resultados relacionados com a estruturação da segurança representam uma fragilidade na capacidade das Ifes na realização das atividades relacionadas com segurança da informação e impactará significativamente nos demais resultados da pesquisa.



Mesmo diante de um quadro deficitário de pessoal para atender as atividades de TIC, a maioria (85,7%) das Ifes afirma que não terceiriza responsabilidades com segurança. Para os que responderam positivamente, as seguintes responsabilidades são terceirizadas: administração e suporte a sistemas de segurança como firewall e IDS (9,5%), toda área/departamento (2,4%), gerência da rede (4,8%), aplicação de patches e atualizações (2,4%) e novos projetos (2,4%).

Política de Segurança

Com relação a Políticas e Normas de Segurança da Informação, 97,6% afirmam que não possuem um documento formalmente desenvolvido e aprovado pela reitoria da instituição. Entretanto, observa-se iniciativas de desenvolvimento a médio prazo.

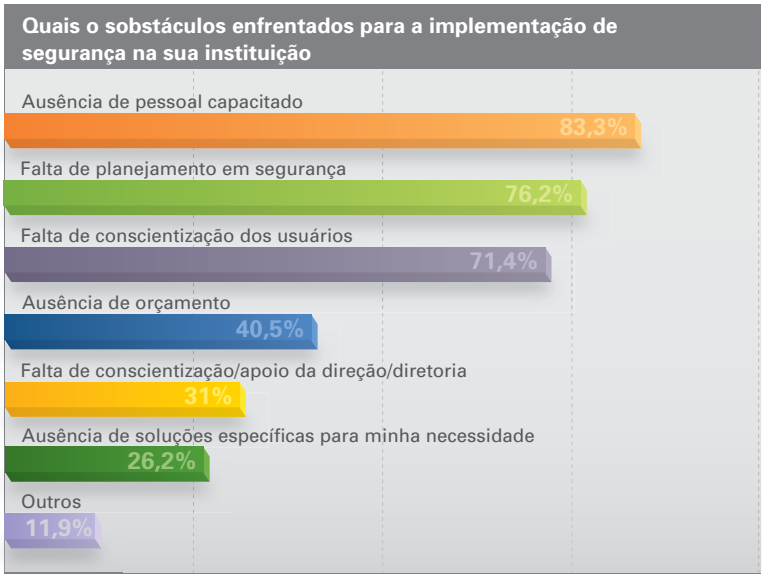
Análise de Riscos e Auditorias

Um total de 92,9% das Ifes não possui um processo de análise de riscos documentado e em operação. Esse número representa uma grande fragilidade na capacidade da instituição em avaliar o nível da segurança e priorizar ações para tratamento dos riscos relevantes ao seu negócio.

Da mesma forma, 88,1% das Ifes não possuem um planejamento formal e anual em segurança da informação que considere, dentre outros pontos, os resultados da análise de risco. Para as instituições que fazem um planejamento de segurança (11,9%), esta iniciativa iniciou recentemente (há menos de 1 ano).

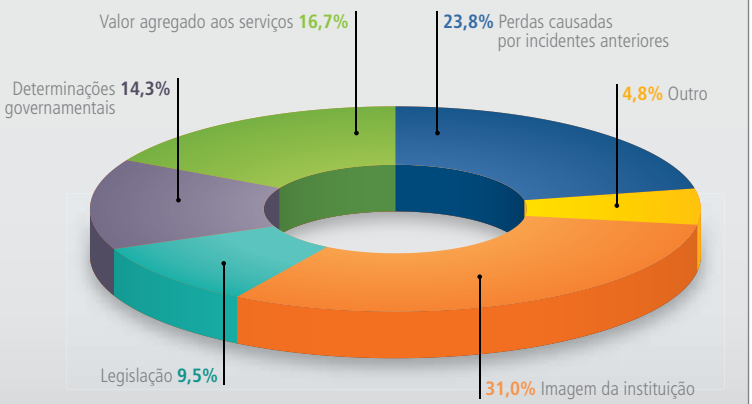
Implementação da segurança

Os principais obstáculos para a implementação da segurança apontados foram ausência de pessoal capacitado (83,3%) e a falta do planejamento de segurança (76,2%).



O maior motivador para a tomada de decisões visando à segurança é o impacto na imagem da instituição causado por incidentes de segurança (31%), seguido pelas perdas causadas por incidentes anteriores (23,8%)

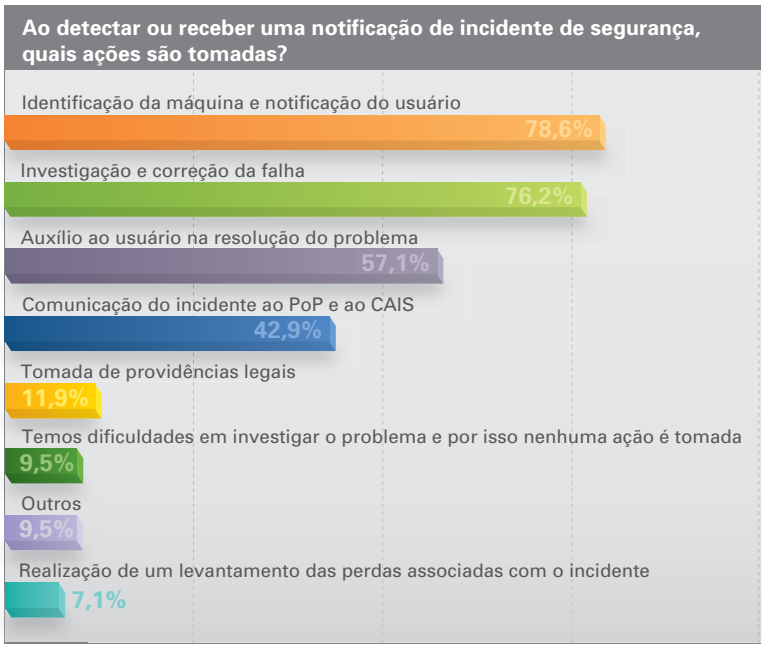
Qual o principal motivador em sua instituição para a tomada de decisões visando a segurança da informação?



Tratamento de Incidentes de Segurança

Um dos aspectos avaliados na pesquisa é a capacidade das Ifes em responder aos incidentes de segurança envolvidos com a instituição. Para tanto, questionou-se a existência de um CSIRT e 81% das Ifes afirmaram que não possuem um CSIRT em operação.

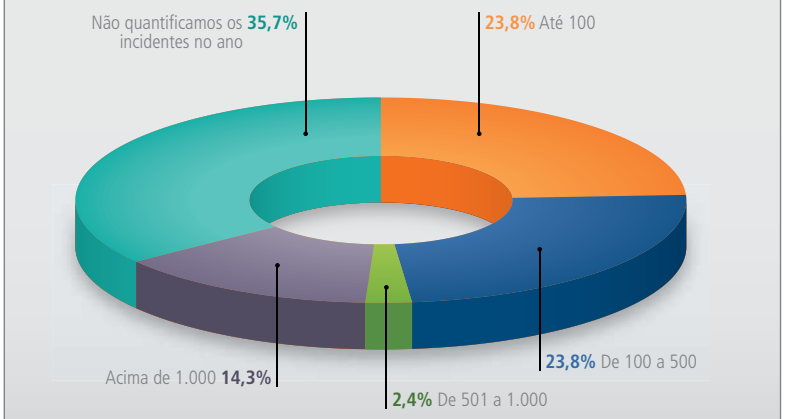
As principais medidas tomadas ao detectar um incidente consistem na identificação da máquina e notificação do usuário (78,6%), investigação e correção da falha (76,2%) e auxílio ao usuário na resolução do problema (57,1%). A carência de profissionais nas Ifes dificulta uma atuação mais efetiva na resolução de incidentes de segurança e no levantamento das perdas associadas com os incidentes que só é realizado em 7,1% das instituições.



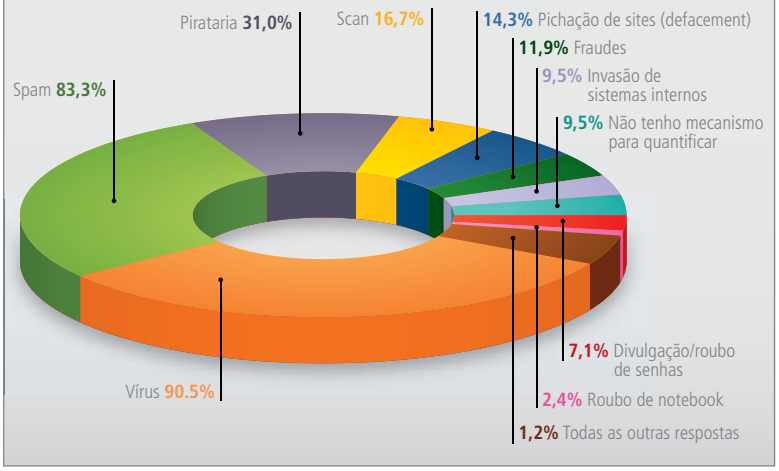
Os principais tipos de incidentes apresentados em 2009 nas Ifes são vírus (90,5%), spam (83,3%) e pirataria (31%). Isto é resultado, dentre outros motivos, da grande quantidade de estações de trabalho e usuários e da dificuldade em implantar políticas únicas de segurança da informação.

Com relação à quantidade de incidentes ocorridos no ano anterior à presente pesquisa, 35,7% das Ifes afirmaram que não quantificam.

Quantos incidentes sua instituição sofreu em 2008?

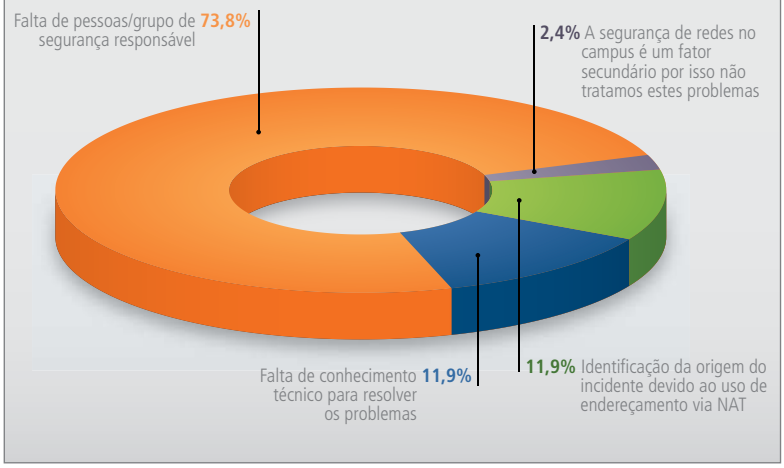


Quais foram os principais incidentes de segurança ocorridos em sua instituição nos últimos 12 meses (assinale 3)



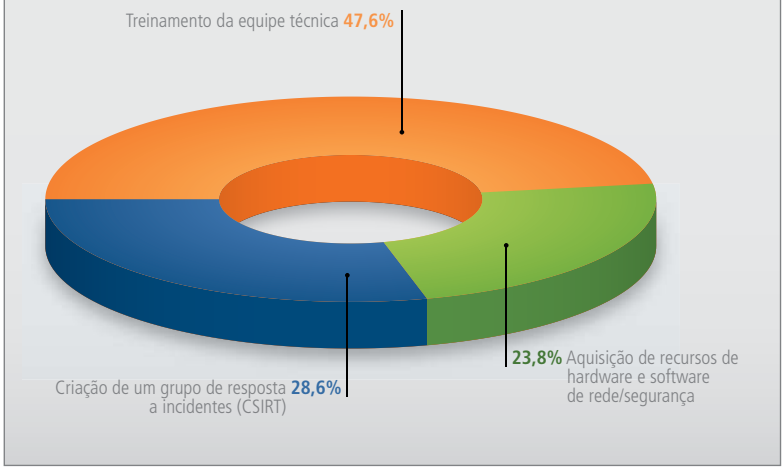
A principal dificuldade apontada pelas Ifes na resolução de incidentes de segurança consistiu na falta de pessoal e grupo responsável (73,8%). A falta de conhecimento técnico (11,9%) e a dificuldade em identificar a origem do incidente (11,9%) também foram apontados na pesquisa. Esta última tem como causa o uso de NAT e a inexistência de mecanismos configurados para identificar qual a máquina que originou um incidente, quando vinda de redes internas.

Qual a principal dificuldade da sua instituição na resolução dos problemas de segurança enfrentados?



Os fatores que mais auxiliariam as instituições na resolução de incidente são treinamento da equipe técnica (47,6%) e a criação de um grupo de resposta a incidentes de segurança (28,6%).

Qual o fator que mais auxiliaria na resolução de incidentes de segurança em computadores no campus?

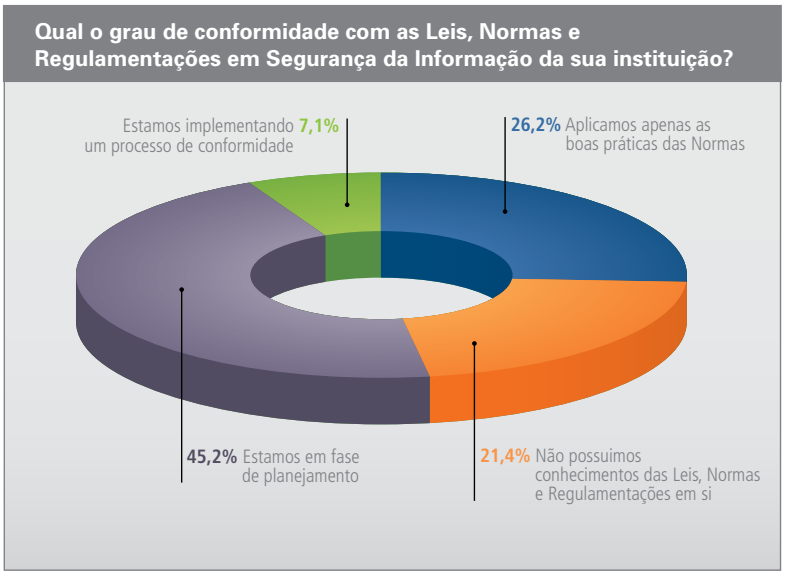


Conformidade

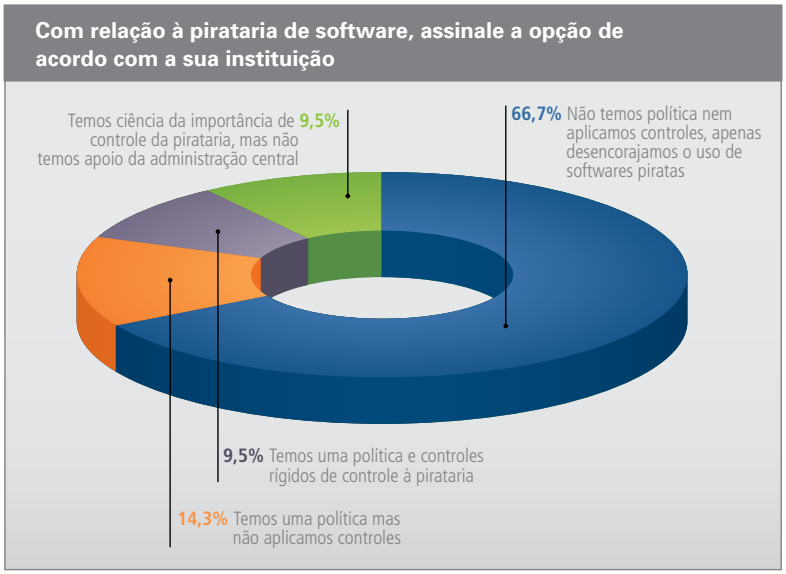
As normas e leis relacionadas à segurança da informação e TIC não tem sido observadas com atenção pelas Ifes. Dois terços das instituições declararam possuir pouco conhecimento sobre o assunto, e ainda não adotaram nenhuma medida específica nesta direção. Apenas 14,3% afirmam possuir conhecimento e estarem em conformidade.

Com relação ao grau de conformidade com as leis, normas e regulamentações em segurança em que as Ifes se encontram, 45,2% afirmaram estar em fase de planejamento; 26,2% afirmaram que apenas aplicam as boas práticas das normas de segurança; 21,4% alegam não possuir conhecimento das mesmas; e 7,1% estão em processo de conformidade.

Qual o grau de conformidade com as Leis, Normas e Regulamentações em Segurança da Informação da sua instituição?



Para as instituições, no processo de conformidade, os documentos apontados como sendo a base de referência para implantação de boas práticas em TIC foram COBIT (9,5%), Novo Código Civil (7,1%) e ISO 27001 (2,4%).



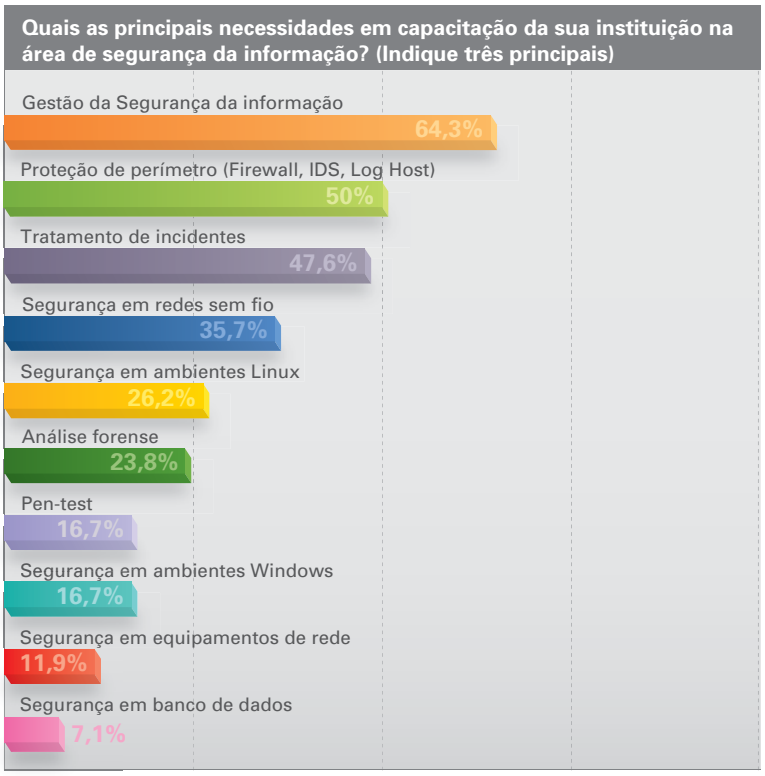
Com relação à pirataria de software, 66,7% das Ifes afirmaram que não possuem políticas e nem aplicam controles para evitar, apenas desencorajam o uso de softwares piratas na instituição. Apenas 9,5%, possuem políticas e controles implantados para a pirataria de software na instituição

Da mesma forma, 61,9% das Ifes não aplicam nenhum controle para evitar o compartilhamento de arquivos protegidos por direito autoral via P2P.

Capacitação

Em termos de capacitação em segurança da informação, 90,5% planejam investir nessa área nos próximos 12 meses. As principais necessidades apontadas pelas Ifes são gestão de segurança da informação (64,3%), proteção de perímetro (50%) e tratamento de incidentes (47,6%).

A grande maioria das Ifes (95.2%) afirma não possuir profissionais certificados em segurança.



Considerações Finais

O CAIS agradece às instituições que participaram desta pesquisa. Uma consolidação preliminar dos dados foi apresentada à comunidade acadêmica e de pesquisa no Workshop de Segurança, coordenado pelo CAIS no âmbito do Seminário de Capacitação e Inovação, em 2009. Na ocasião, o CAIS teve a oportunidade de recolher um primeiro retorno de representantes desta comunidade presentes no evento.

Os resultados obtidos com a presente pesquisa devem subsidiar o planejamento de ações em segurança da RNP no âmbito acadêmico, assim como já foram utilizados para o planejamento de ações para 2011. Uma próxima pesquisa deverá ocorrer neste ano, abrangendo um número maior de instituições de ensino e pesquisa. Esta também permitirá avaliar comparativamente os resultados e oferecer indicadores que permitam medir a efetividade das ações.

Ministério da Ciência e Tecnologia
Ministério da Educação
Ministério da Cultura

Rede Nacional de Ensino e Pesquisa
Nelson Simões
Diretor-Geral

Diretoria de Serviços & Soluções
José Luiz Ribeiro Filho
Diretor

Centro de Atendimento a Incidentes de Segurança (CAIS)
Liliana Velásquez
Gerente

Revisão
Gerência de Comunicação Corporativa

Projeto gráfico e diagramação
Tecnodesign

Contato: +55 19 3787-3300

Ministério da
Cultura

Ministério da
Educação

Ministério da
Ciência e Tecnologia