Dia a dia de um IRT - A Experiência do CAIS

Jacomo D. B. Piccolini – jacomo@cais.rnp.br

Centro de Atendimento a Incidentes de Segurança

CAIS / RNP

Maio de 2001

© 2001 – RNP

RNP

Sumário

Introdução

A Experiência do CAIS

- Dia a dia de um IRT
- Como tratar incidentes?
- Como agir quando um incidente parte de sua rede?
- Como reportar incidentes para a sua rede?
- Como agir em casos de invasão?

Sumário

A Experiência do CAIS (cont.)

- SPAM
- Medidas Preventivas
- Aspectos Legais
- Contatos
- Referências

Introdução

RNP e CAIS

- RNP Rede Nacional de Pesquisa (MCT/CNPq)
- **CAIS**: Centro de Atendimento a Incidentes de Segurança
  - Criado em 1997
  - Missão: registro e acompanhamento de problemas de segurança no backbone e PoPs da RNP, além da disseminação de informações sobre ações preventivas relativas a segurança.
  - 1999: ênfase nas atividades preventivas
  - Escopo de atuação: Redes não comerciais conectadas ao backbone da RNP.

Atividades do CAIS

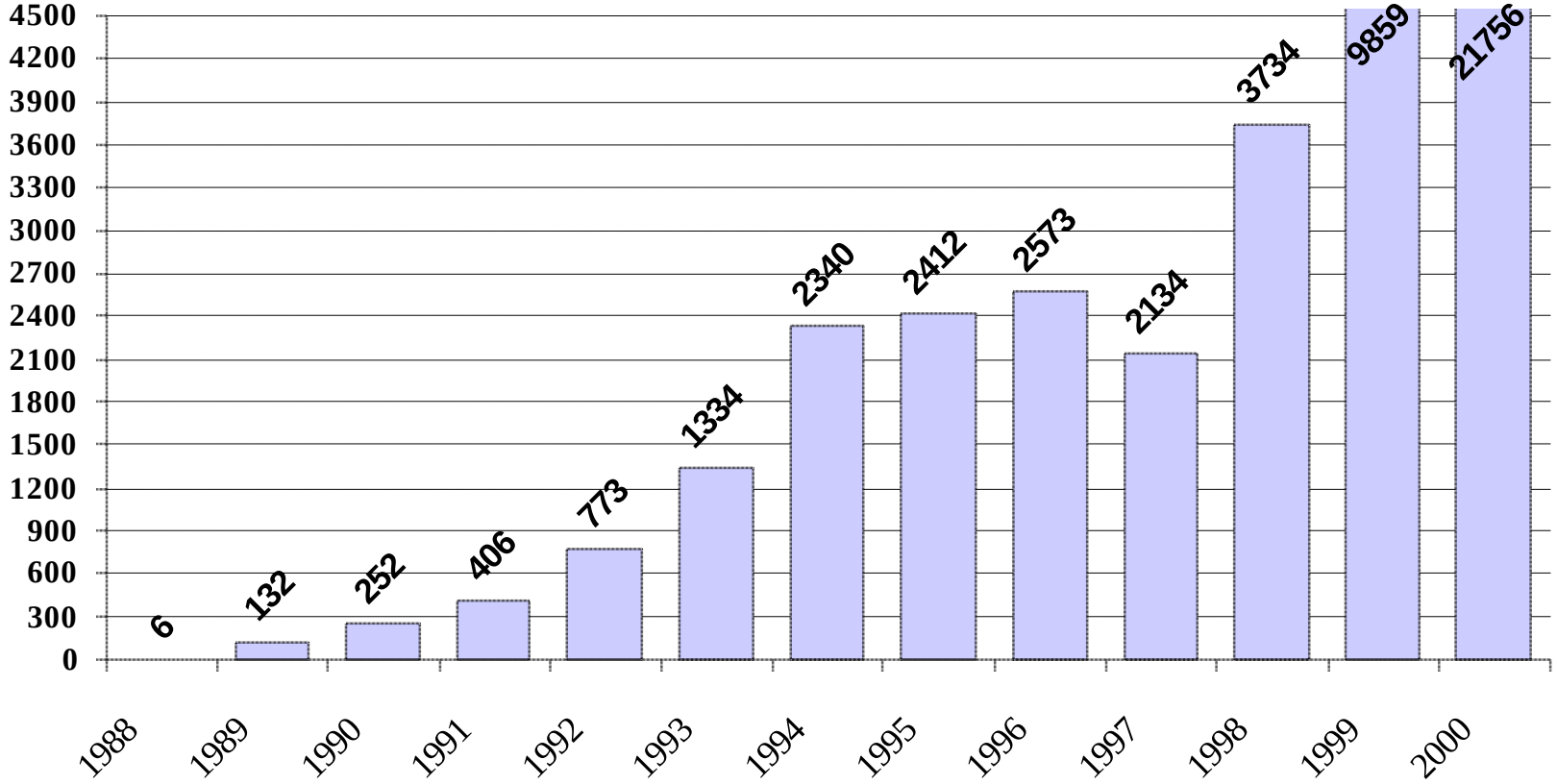
- As atividades do CAIS são:
  - Tratamento de incidentes de segurança
  - Divulgação de alertas e recomendações
  - Disseminação de informações relacionadas a segurança
  - Elaboração de políticas de segurança para a RNP
  - Testes de ferramentas de segurança
  - Treinamento na área

Atividades do CAIS

- Projetos do CAIS:
  - NTP stratum 1 na RNP
  - Auditorias periódicas
  - Políticas de segurança
  - Consultorias

Panorama na Área de Segurança

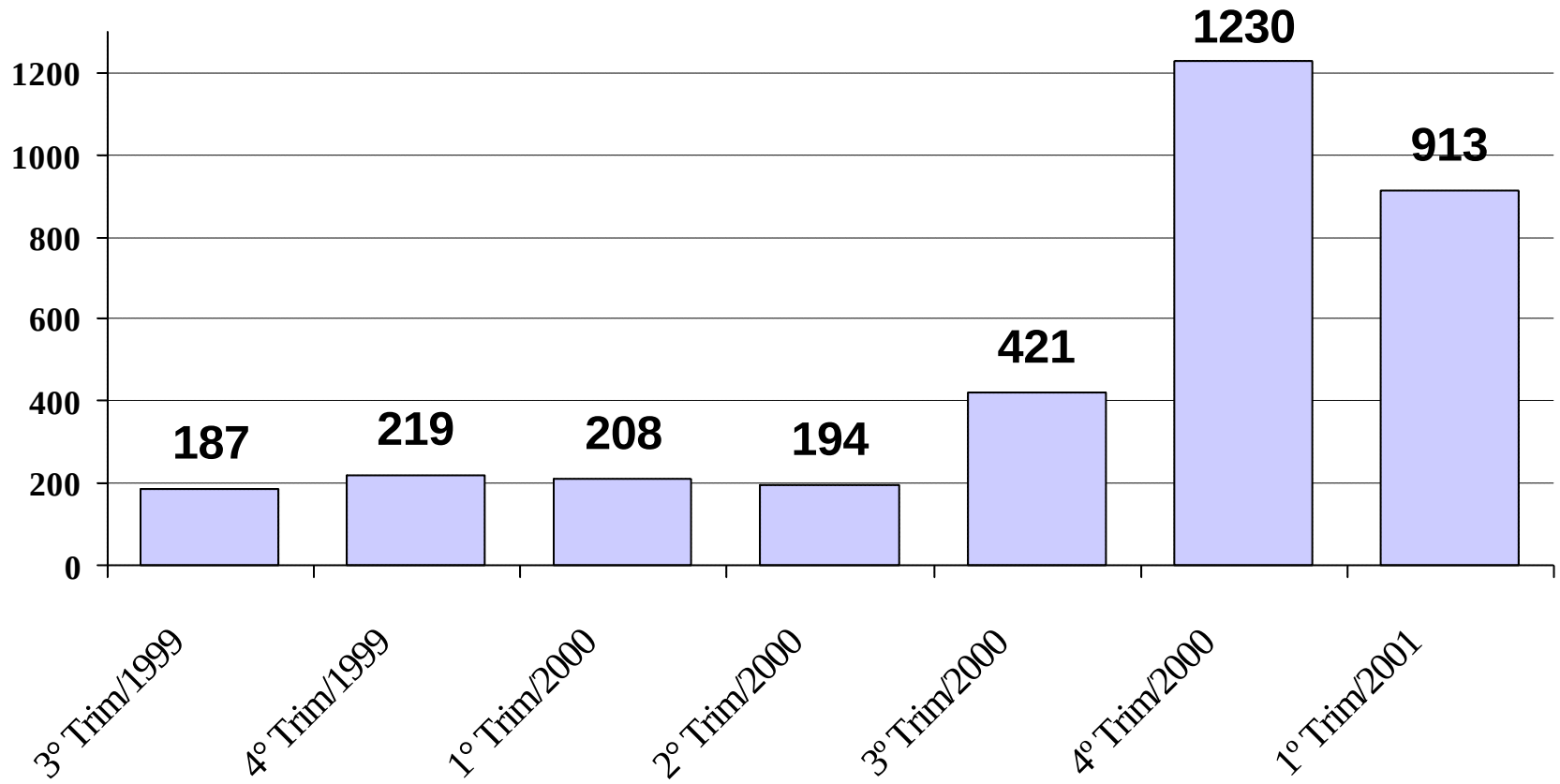
- Estatísticas do CERT/CC



Fonte: www.cert.org/stats/cert_stats.html

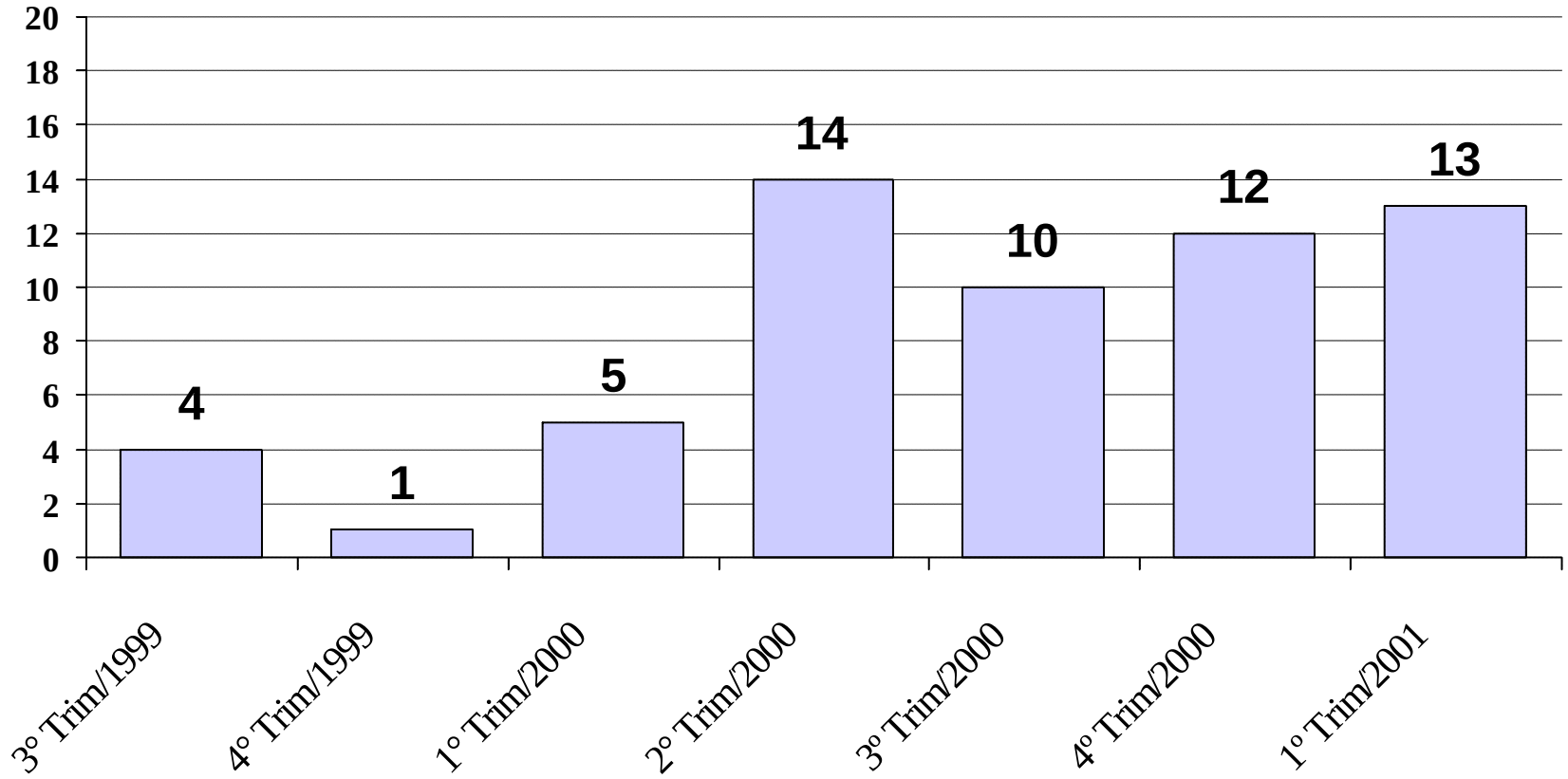
Panorama na Área de Segurança

- Estatísticas do CAIS:



Panorama na Área de Segurança

- Ataques a Sites de Universidades



Panorama na Área de Segurança

- No ano 2000
  - Troca de páginas web
  - SPAM e Relay
  - DoS (Negação de serviço)
  - Scans em geral
- No ano 2001
  - Scans em geral
  - SPAM e Relay
  - Troca de páginas web
  - Worms

Dia a dia de um IRT

- ***IRT: Incident Response Team***
- No tratamento de incidentes de segurança, são premissas básicas:
  - **Rapidez**
  - **Sigilo**
  - Rede de contatos eficiente
  - Documentação e histórico
  - Apoio da gerência e/ou coordenação imediata
  - Reportar o incidente

Como tratar incidentes?

- Ter uma pessoa ou um grupo designado para Segurança de redes
- Implementar as contas previstas no RFC 2142: **abuse@dominio**, **security@dominio, postmaster@dominio**.
- Tarefas básicas:
  - esclarecer, orientar e conscientizar administradores e usuários de sua rede corporativa para os assuntos relacionados a segurança
  - receber notificações de segurança das diversas áreas da Organização, encaminhá-las aos orgãos competentes, acompanhando o incidente até que o mesmo seja esclarecido.

Como tratar incidentes?

- Tarefas básicas: (cont.)
  - receber denúncias de incidentes partindo de sua rede, investigar, garantir que providências sejam tomadas internamente e **responder** aos reclamantes.
  - cooperar com outros grupos, contatos responsáveis por segurança e polícia, visando o cruzamento de informações e a colaboração nas investigações.

Como agir quando um incidente parte de sua rede?

- Se a sua rede for origem de ataques ...
  - Fazer uma auditoria minuciosa na máquina de onde partiu o incidente e nas demais máquinas de sua rede.
  - Se a máquina estiver invadida, esta deverá estar sendo usada como base de ataques. Agir seguindo as recomendações em caso de invasão.
  - Se o incidente partiu de usuário interno, então o mesmo deve ser enquadrado nas AUPs

Como agir quando um incidente parte de sua rede?

- Se a sua rede for origem de ataques ...(cont.)
  - Nos casos em que a Polícia tenha sido envolvida, é comum ter que passar os dados do usuário, mediante mandato judicial.
  - Documentar o incidente
  - Identificar a vulnerabilidade explorada, corrigindo-a.
  - Adequar a política de segurança

Como reportar incidentes para sua rede?

- E se a sua rede for alvo de ataques?
  - Enviar uma notificação do incidente ao contato técnico pela rede origem do ataque e/ou para o grupo de segurança responsável.
  - A notificação deve conter o tipo de atividade detectada, os impactos ou danos causados, data, horário, Timezone (GMT-), logs correspondentes, providências esperadas.
  - Copiar sempre o grupo de segurança responsável pela sua rede, se houver, para que ele possa atuar se necessário.

Como agir em caso de invasão?

- Em caso de invasão, o CAIS recomenda:
  - Fazer um *mirror* do disco comprometido.
  - Reinstalar **totalmente** o sistema.
  - Fechar todos os serviços não utilizados.
  - Fazer uma revisão de contas e senhas.
  - Verificar **todas** as máquinas da rede
  - Analisar os logs e arquivos suspeitos
  - Contatar os orgãos competentes

SPAM

- SPAM é um abuso, e **não** ataque! SPAM **não** faz parte do escopo de atuação do CAIS. O CAIS apenas orienta e recomenda.
- RFC 2142: implementar as contas abuse@ e postmaster@
- Em caso de **SPAM partindo** de sua rede:
  - Advertir e punir o usuário, de acordo com as AUPs
  - Responder para o reclamante
- Em caso de **SPAM para** a sua rede:
  - Enviar reclamação formal para os contatos técnicos pelo domínio origem do SPAM e/ou para ***abuse@dominio***.
  - Anexar a reclamação, o header completo da mensagem de SPAM

SPAM

- Em caso de **SPAM para** a sua rede: (cont.)
  - Anexar a reclamação, o conteúdo da mensagem de SPAM somente se incluir informações relevantes para uma possível investigação.
  - Em caso de uso de relay para o envio de SPAM, deve-se copiar a reclamação para o contato técnico pelo domínio usado como relay e/ou correspondente ***abuse@,*** copiando o grupo de segurança responsável.
  - Enviar cópia para o MAPS: ***relays@mail-abuse.org***, incluindo no corpo do e-mail ***Relay: <IP-do-servidor>***

Medidas preventivas

- Análise de logs
- Investigação de qualquer tipo de comportamento anômalo na rede ou nos serviços
- IDS
- Manter sistemas operacionais e aplicativos atualizados com as últimas versões e patches disponíveis.
- Acompanhar os alertas de segurança relacionados aos sistemas e aplicativos usados em sua rede.
- Auditorias periódicas
- Políticas de segurança

Aspectos Legais

Lei Nº 9.610, de 19 de Fevereiro de 1998.

Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências.

http://www.planalto.gov.br/ccivil_03/Leis/L9610.htm

Lei Nº 9.609 , de 19 de Fevereiro de 1998.

Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.

http://www.planalto.gov.br/ccivil_03/Leis/L9609.htm

Aspectos Legais

Lei Nº 9.296, de 24 de Julho de 1996 (Sobre a Interceptação de documentos eletrônicos)

Regulamenta o inciso XII, parte final, do art. 5º. da Constituição Federal.

http://www.planalto.gov.br/ccivil_03/Leis/L9296.htm

Lei Nº 9.279, de 14 de Maio de 1996.

Regula direitos e obrigações relativos à propriedade industrial.

http://www.planalto.gov.br/ccivil_03/Leis/L9279.htm

Aspectos Legais

Decreto No 3.587, de 5 de Setembro de 2000.

Estabelece normas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal - ICP-Gov, e dá outras providências

http://www.planalto.gov.br/ccivil_03/decreto/D3587.htm

Decreto Nº 3.505, de 13 de Junho de 2000

Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm

Aspectos Legais

Decreto Nº 2.556, de 20 de Abril de 1998

Regulamenta o registro prevista no art. 3º da Lei nº 9.609, de 19 de fevereiro de 1998, que dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.

http://www.planalto.gov.br/ccivil_03/decreto/D2556.htm

Aspectos Legais

Projeto de Lei Nº 3.533, de 2000

Dispõe sobre a proteção de informação não divulgada submetida para aprovação da comercialização de produtos e dá outras providências.

http://www.planalto.gov.br/ccivil_03/Projetos/PL/2000/msg1235-00904.htm

a) Projetos de Lei do Senado

Projeto de Lei Nº 76, de 2000 (Do Senador Renan Calheiros)

Define e tipifica os delitos informáticos, e dá outras providencias

http://www.senado.gov.br/web/senador/renancal/renancal.htm

Aspectos Legais

Projeto de Lei Nº 234, de 1996 (Do Senador Júlio Campos)

Define crimes contra a inviolabilidade de comunicação de dados de computador.

b) Projetos de Lei da Câmara de Deputados

Projeto de Lei Nº 3016, de 2000 (Do deputado Antonio Carlos Pannunzio)

Dispõe sobre o registro de transações de acesso a redes de computadores destinadas ao uso público, inclusive a Internet.

Aspectos Legais

Projeto de Lei N° 1.589, de 1999 (Do Deputado Luciano Pizzatto e outros)

Dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital, e dá outras providências.

Projeto de Lei N° 84, de 1999 (Do Deputado Luiz Piauhylino, 1999)

Dispõe sobre os crimes cometidos na área de informática, suas penalidades e outras providências.

Projeto de Lei Nº 1.713, de 1996 (Do Deputado Cássio Cunha Lima)

Dispõe sobre o acesso, a responsabilidade e os crimes cometidos nas redes integradas de computadores e dá outras providências.

Aspectos Legais

* Ministério de Desenvolvimento, Indústria e Comercio Exterior (MDIC)

Portaria Nº 58 de 18 de maio de 1998. Sobre o Comercio Eletrônico (De José Botafogo Gonçalves)

* Ministério das Comunicações (MC)

Lei Nº 9.472, de 16 de Julho de 1997. Lei Geral das Telecomunicações Brasileiras

* Ministério de Ciência e Tecnologia (MCT)/Ministério das Comunicações

Portaria Interministerial Nº 147, de 31 de Maio de 1995. Sobre a livre competição entre provedores

Aspectos Legais

Comitê Gestor

Resolução Nº 001/98 (14.04.98)

O documento é um resumo das regras atualmente adotadas pela FAPESP para o registro de domínios no País, bem como as normas para a cobrança e pagamento das taxas.

http://www.cg.org.br/regulamentacao/resolucao001.htm

Resolução Nº 002/98 (14.04.98)

Delega à FAPESP as atividades de registro de nomes de domínio, distribuição de endereços IPs e sua manutenção na Internet.

http://www.cg.org.br/regulamentacao/resolucao002.htm

Aspectos Legais

NBR 11420/90

NBR 11421/90

NBR 11514/91

NBR 11515/91

NBR 11584/91

NBR 12896/93

NBR 12964/93

Aspectos Legais

Constituição do Brasil

CRIMES DE INFORMÁTICA - DISPOSITIVOS RELACIONADOS:

TÍTULO II

Dos Direitos e Garantias Fundamentais

CAPÍTULO I

Dos Direitos e Deveres Individuais e Coletivos

Art. 5.º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

Aspectos Legais

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Contatos

- Cooperação com grupos de segurança:
  - No Brasil: NBSO, Security UNICAMP, Cert-RS.
  - No Exterior: CERT/CC, JPCERT, DFNCert, IrisCERT, AusCERT, dentre outros.
- Polícia Federal: SAAC, Setor de Apuração de Crimes por Computador, saac@nic.br
- Delegacias Estaduais:
  - Policia Civil de São Paulo: Setor de Crimes pela Internet: webpol@policia-civ.sp.gov.br

Referências

- Home Page do CAIS: www.rnp.br/cais
- Projeto NTP Stratum 1: www.rnp.br/cais/ntp
- News Generation: www.rnp.br/newsgen
- "Computer Security Incident Handling Step by Step" Stephen Northcutt; The SANS Institute, Version 1.5, 1998
- RFC 2142: Mailbox Names for Common Services, Roles and Functions
- CERT/CC: www.cert.org
- SANS: www.sans.org

Referências

- NBSO: www.nic.br
- Security Unicamp: www.security.unicamp.br
- ORBS: www.orbs.org
- MAPS: www.mail-abuse.org
- RFC 1281 "Guidelines for the Secure Operation of the Internet" R. Pethia; S. Crocker; B. Fraser; 1991
- RFC 2196 "Site Security Handbook" B. Fraser; 1997