



Grupo de Resposta a Incidentes de Segurança

GRIS

O que é um incidente de segurança?

*“Qualquer evento **adverso**, confirmado ou sob suspeita, que pode ameaçar a segurança dos sistemas de computação ou das redes de computadores.”*



O que é um incidente de segurança?

*“Qualquer evento **adverso**, confirmado ou sob suspeita, que pode ameaçar a segurança dos sistemas de computação ou das redes de computadores.”*

- OU -

“O ato de violar uma política de segurança, explícita ou implícita.”



O que é um incidente de segurança?

Exemplos:

- Tentativas (com ou sem sucesso) de ganhar acesso não autorizado a sistemas ou a seus dados



O que é um incidente de segurança?

Exemplos:

- Tentativas (com ou sem sucesso) de ganhar acesso não autorizado a sistemas ou a seus dados
- Interrupção indesejada ou negação de serviço



O que é um incidente de segurança?

Exemplos:

- Tentativas (com ou sem sucesso) de ganhar acesso não autorizado a sistemas ou a seus dados
- Interrupção indesejada ou negação de serviço
- Uso não autorizado de um sistema para processamento ou armazenamento de dados



O que é um incidente de segurança?

Exemplos:

- Tentativas (com ou sem sucesso) de ganhar acesso não autorizado a sistemas ou a seus dados
- Interrupção indesejada ou negação de serviço
- Uso não autorizado de um sistema para processamento ou armazenamento de dados
- Modificações nas características de hardware, firmware ou software de um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema



O GRIS

CSIRT formalizado para receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança dentro da UFRJ

- Centralização e organização no tratamento a incidentes
- Velocidade na resposta



O GRIS

Alguns laboratórios já contemplados:

- Laboratório de Informática da Graduação (LIG - IM)
- Laboratório de Matemática Aplicada (LABMA - IM)
- Laboratório do Curso de Informática (LCI - IM)
- Núcleo de Tecnologia Educacional para a Saúde (NUTES - CSS)
- Núcleo de Estudos do Quaternário e Tecnógeno (NEQUAT - IGeo)
- Laboratório de Gestão do Território (LAGET - IGeo)



GRIS – Muito mais que um CSIRT

- Grupos de estudo e seminários internos
- Fomento à pesquisa e produção de
 - Artigos (populares e técnico/científicos)
 - Tutoriais
 - Ferramentas



GRIS – Projetos em Andamento

Labrador-IDS

```
xterm
analizando arquivo "/bin/telnet"... OK
analizando arquivo "/bin/loadkeys"... OK
analizando arquivo "/bin/umount"... OK
analizando arquivo "/bin/dircolors"... OK
analizando arquivo "/bin/lsmold.old"... OK
analizando arquivo "/bin/gawk-3.1.3"... OK
analizando arquivo "/bin/ypdomainname"... OK
analizando arquivo "/bin/getoptprog"... OK
analizando arquivo "/bin/bzip2recover"... OK
analizando arquivo "/bin/Autoscan"... OK
analizando arquivo "/bin/bunzip2"... OK
analizando arquivo "/var/www/htdocs/index.html"... !!! FALHOU !!!
[teste de MD5] - Arquivo foi substituído ou modificado!
valor original: ac8b12cbeb14402d8bf9d597cefa417d
valor atual: 3d0eff53cb4b0e6fef761a224219bb1b

Arquivo /var/www/htdocs/index.html pode ser restaurado do backup. Gostaria que e
u tentasse? Preciso de um 'sim' completo digitado aqui, já que vou sobrescrever
um arquivo com uma versão anterior que pode causar perda de dados ou afetar o fu
ncionamento correto do sistema (caso o atual seja um arquivo legítimo). De qualq
uer forma, é melhor que você primeiro crie uma cópia de backup do arquivo atual
manualmente, só por garantia. Então, devo restaurar?
```



GRIS – Projetos em Andamento

FerrO

- ♦ Varredura de portas
- ♦ Detecção de vírus
- ♦ Detecção de links quebrados
- ♦ Proxy anônimo



GRIS – Projetos em Andamento

Tamoio BSD

- Live-CD seguro baseado em OpenBSD
- Ferramentas de RI e auditoria
- Análise em redes isoladas ou com configurações específicas
- Execução de serviços provisórios (sshd, httpd) em máquinas comprometidas



GRIS – Projetos em Andamento

Truta

- Análise de Golpes (Phishing Scams)
- Busca por Golpes documentados
- Educação





Dúvidas?