DIRETRIZES DE AÇÕES REFERENTES A INCIDENTES DE SEGURANÇA ENVOLVENDO INSTITUIÇÕES DA REDERIO DE COMPUTADORES/FAPERJ

Esta política abrange um conjunto de práticas e procedimentos com a intenção de melhor tratar os incidentes de segurança referentes as instituições pertencentes a RedeRio de Computadores (Sistema Autônomo 2715) e que possam provocar a perda de dados ou afetar a integridade, disponibilidade e confidencialidade das informações acadêmicas e governamentais.

- **Objetivos**

Assegurar que os eventos de segurança de informação sejam tratados de forma efetiva, permitindo o adequado registro, investigação e tomada de ação corretiva em tempo hábil para mitigar o impacto negativo sobre o tráfego de dados no backbone da RedeRio, evitar a propagação de códigos maliciosos e impedir danos a imagem da instituição.

- **Classificação dos Incidentes de Segurança**

1. Virus/Worms/Malwares/Bots
2. Violação de direitos autorais
3. Mensagens eletrônicas com Spam/Phishing
4. Páginas Web desfiguradas
5. Ataques de força bruta – Probes
6. DDOS – negação de serviços
7. Invasão de hosts
8. Outros

- **Procedimentos**

O procedimento padronizado para o tratamento de incidentes de segurança compreende as seguintes etapas:

A – Por parte da equipe de segurança da Coord. de Engenharia de Operações (CEO/RedeRio):

- Recepção da denúncia ou alerta de atividade maliciosa;
- Análise da gravidade do incidente;
- Envio da denúncia para os responsáveis da Instituição envolvida;
- Acompanhamento das ações tomadas pela Instituição envolvida;
- Análise crítica e medidas corretivas;
- Em caso de não resposta sobre o incidente, a CEO poderá tomar medidas no sentido de evitar um incidente que prejudique o bom funcionamento de toda a rede;

B – Por parte dos responsáveis pelas redes das Instituições:

- Receber e analisar as notificações dos incidentes com prioridade alta;
- Tomar as medidas necessárias para interrupção da atividade maliciosa;
- Reportar a CEO/RedeRio o desfecho do incidente;

- **Disposições finais**

A RedeRio de Computadores/FAPERJ reserva o direito de revisar estas diretrizes periodicamente para adaptá-la às necessidades mais atuais de segurança de sistemas de informação.