

# Consulta Reitoria 2022

## Auditoria do Sistema

07/04/2022



Universidade  
Estadual de  
Ponta Grossa

# Segurança

- Combinação de mecanismos de segurança física e lógica e documentos
- Física
  - Lacres, fechaduras e ambientes controlados
- Lógica
  - Mecanismos do sistema operacional, banco de dados e sistema de votação
- Documentos
  - Atas, formulários, assinaturas, etc

# Garantia da não-identificação do voto do eleitor

- Ao depositar o voto, são feitas duas operações independentes em uma única transação para garantir a atomicidade da execução da mesma
- As duas operações independentes são:
  - Incluir voto  
Insert na tabela 'votação'
  - Marcar que o eleitor votou  
Update na tabela 'urna\_votou'

# Garantia da não-identificação do voto do eleitor

- Ao término da eleição a soma dos votos depositados e das abstenções que deve obrigatoriamente corresponder ao total de eleitores de cada urna
  - O total de votos de cada urna deve corresponder a quantidade de assinaturas de eleitores no caderno de votação
  - As abstenções de cada urna devem corresponder as assinaturas em branco no caderno de votação de cada urna

# Garantia da inviolabilidade do voto

- É implementada uma cadeia de confiança com elementos físicos e lógicos para garantir a geração de evidências que impossibilitem qualquer adulteração
- Esse processo vem sendo desenvolvido e aprimorado nos últimos 12 anos
- Essas evidências foram projetadas para jamais identificar o voto do eleitor
  - Isso inclusive aumenta a complexidade dessa cadeia de confiança

# Garantia da inviolabilidade do voto

1. O código do Sistema é auditado e a hash de todos os arquivos é gerada – impossibilita adulteração do código
2. O SO do servidor é auditado e o acesso remoto (SSH) é desabilitado e regras de firewall são habilitadas
3. O servidor é lacrado fisicamente e a partir desse momento, todos os procedimentos de lacre físico (nos dias de votação e para a apuração) são realizados com ata e presença dos peritos das chapas

# Garantia da inviolabilidade do voto

4. A auditoria do SGBD junto com a auditoria do código impossibilita qualquer forma de adulteração na tabela votacao
5. Todos os votos precisam da assinatura física do eleitor no caderno de votação
6. A lista de abstenções é divulgada junto com o resultado
7. Em qualquer momento pode ser feita uma auditoria de código (verificação de hash) ou de registros na auditoria do SGBD

# Garantia da inviolabilidade do voto

8. Ao término da apuração, os discos do servidor são lacrados e permanecem íntegros e invioláveis para auditoria posterior caso necessário

# Auditoria do SGBD

- Habilidade auditoria nativa do SGBD
- Garante integridade da auditoria
  - Processo intrínseco do SGBD
  - Não é possível apagar registros

# Opções de auditoria habilitadas (SGBD)

- Comandos
  - Alter
  - Create
  - Drop
  - Dump
  - Grant
  - Load
- Todos os comandos do usuário 'sa'
  - Em operação normal não deverá ter nenhum registro na auditoria do usuário 'sa', salvo tarefa de indexação automática

# Opções de auditoria que NÃO foram ativadas

- Não foram ativadas para ter a garantia de não identificar o voto
  - all
  - cmdtext
  - insert
  - select
  - table\_access
  - update
  - view\_access

# Opções de auditoria habilitadas – tabela ‘votacao’

- Durante a votação a tabela ‘votacao’ deve obrigatoriamente aceitar somente comandos ‘insert’ de novos votos
- Durante a votação, em nenhuma hipótese, a tabela pode ter comandos ‘update’ ou ‘delete’
- Somente para essa tabela, os comandos ‘update’ e ‘delete’ tem a auditoria habilitada
  - Isso não identifica o voto, pois a tabela ‘votacao’ tem apenas o registro do voto e não do código do eleitor

# Backup do SGBD

- É realizado a cada 15 minutos
- Feito pelo cron do Linux
  - Usuário do sybase 'backup' que somente pode executar dump
  - Não tem nenhum grant no database 'eleição'

# Mensagens que o SO envia

- Syslog do SO para servidor central
  - Procedimento padrão de segurança
- Coleta SNMP
  - Métricas de desempenho: cpu, memoria, carga, rede

# Mensagens que o sistema envia

- Para permitir suporte da equipe técnica durante a votação
  - Abertura de urna
  - Finalização de urna
- A cada 15 minutos (5,20,35,50)
  - Count dos votos depositados

# Auditoria do SO

- Registros completos do estado do computador
- Registros de logon de usuários
- Registro de acesso a aplicação
  - Acesso ao servidor web

# Checklist dia da auditoria

- Alterar senhas
  - Particionar as senhas pelos auditores e comissão eleitoral
- Informar os procedimentos nos dias de votação
- Gerar a hash de todos os arquivos do sistema e incluir como anexo da ata da auditoria

# Checklist dia da auditoria

- Auditoria do SO
  - Bloqueio do ssh
  - Configuração do firewall
  - Remover a pasta eleicoes/cadastro (sem uso)
- Auditoria do SGBD
  - `sp_displayaudit`
- Auditoria do código do sistema de votação e apuração

# Checklist dia da auditoria

- Lacre físico do computador-servidor
- Trancar e lacrar o rack onde o computador-servidor ficará alocado
- Trancamento da sala onde o rack está
- Lacre em envelope inviolável das chaves da sala e do rack
- Lavrar ata das ações realizadas assinada pelos presentes

# Agenda

- 9/4 – Sábado – 16h – NTI
  - Remover lacre do servidor e ligar para iniciar a votação nos polos/campi avançados
- 9/4 – Sábado – 21h – NTI
  - Desligar e lacrar servidor
- 13/4 – Quarta-feira – 8h – NTI
  - Remover lacre do servidor e ligar para iniciar a votação em Ponta Grossa

# Agenda

- 13/4 – Quarta-feira – 21h – NTI
  - Desligar e lacrar servidor
- 13/4 – Quarta-feira – 22h – Ginásio
  - Remover lacre do servidor e ligar para a apuração
  - Após apuração lacre dos discos do servidor

# Agenda

- A presença dos peritos das chapas é requerida em todos os eventos da agenda
- As datas da agenda poderão ser alteradas nos casos previstos pelo Art. 50 da Res. Univ 36/2009

# Caso de falha/problema

- Poderá ser necessário, a qualquer momento, intervenção no computador-servidor caso haja problema no sistema de votação
  - Será necessária a presença dos auditores e membros da comissão eleitoral para que sejam removidos os lacres
  - Será feita ata do ocorrido e log de todos os comandos executados

**Luiz Gustavo Barros   Vladimir Alexandrino de Souza**

**Núcleo de Tecnologia da Informação  
Universidade Estadual de Ponta Grossa**