Relatório Técnico de Auditoria de Segurança da Informação

SEMGE / DPR

Período: Auditoria Interna - Logs de Acesso

1. Introdução

Com o aumento da demanda por serviços públicos digitais, a segurança da informação tornou-se um pilar essencial para garantir a integridade, confidencialidade e disponibilidade das informações. Este relatório apresenta os resultados da auditoria interna realizada na Diretoria de Previdência - DPR, com foco na análise de logs de acesso dos sites e servidores hospedados, conforme os requisitos da Política de Segurança da Informação – PSI

2. Objetivo

O objetivo principal desta auditoria foi verificar a conformidade dos processos de geração, armazenamento e análise de logs de acesso, além de identificar possíveis vulnerabilidades e propor melhorias para o monitoramento proativo dos sistemas.

3. Escopo da Auditoria

3.1. A auditoria abrangeu os seguintes aspectos:

- Integridade e disponibilidade dos logs;
- Análise de padrões de acesso;
- Conformidade com a PSI;

3.2. Os ambientes auditados foram:

- sisprev.salvador.ba.gov.br;
- fpg.salvador.ba.gov.br;
- previdencia.salvador.ba.gov.br;
- portalprevidencia.salvador.ba.gov.br;

3.3. Arquivos de logs analisados:

- LogonSessionsFPG.txt;
- LogonSessionsPREVIDENCIA.txt;
- LogonSessionsPREVISPRD.txt;
- LogonSessionsPREVISPRTL.txt;

4. Resultados da Auditoria

4.1. Geração e Armazenamento de Logs:

4.1.1 Adequação do Sistema: Os logs de acesso são gerados e armazenados de forma centralizada no Data Center da COGEL, garantindo a integridade e a disponibilidade dos dados;

4.1.2 Formatos e Padrões: Os logs são gerados em formatos padronizados, facilitando a análise e a correlação de eventos;
4.1.3 Infraestrutura de Armazenamento: A infraestrutura de armazenamento é dimensionada para suportar o volume de logs gerados, garantindo a retenção adequada dos dados;

4.2. Retenção de logs:

4.2.1 Conformidade com a PSI: O período de retenção de 90 dias atende aos requisitos estabelecidos na PSI, garantindo a disponibilidade dos logs para fins de auditoria e investigação;

4.2.2 Políticas de Retenção: As políticas de retenção de logs são documentadas e revisadas periodicamente, garantindo a conformidade com as regulamentações e os padrões aplicáveis;

4.3. Backup de Logs:

4.3.1 Automatização do Backup: Os backups dos logs são realizados diariamente de forma automatizada, juntamente com a máquina virtual, garantindo a proteção dos dados contra perdas e falhas;

4.3.2 Políticas de Backup: As políticas de backup são documentadas e testadas regularmente, garantindo a integridade e a disponibilidade dos backups, além de estar em conformidade com o as orientações do PSI;

4.4. Controle de acesso aos Logs:

4.4.1 Restrição de Acesso: O acesso aos logs é restrito ao suporte avançado do Data Center (COGEL), exigindo a abertura de chamado para garantir o controle e a rastreabilidade dos acessos;

4.4.2 Auditoria de Acesso: Os acessos aos logs são auditados e registrados, garantindo a rastreabilidade e a responsabilização;

4.5. Análise de Padrões de Acesso:

4.5.1 A maioria dos acessos são realizados por usuários legítimos e dentro do horário comercial;

4.5.2 Não foram detectados acessos fora do horário normal (00:00 às 04:00);

4.5.3 No sistema FPG, foi identificado um acesso pelo usuário "root" com as seguintes características:

- Origem do Acesso: pts/0 (pseudo-terminal, indicando acesso remoto via SSH).
  Endereço IP: x.x.x.12;

- Data e Hora: Quarta-feira, 24 de abril de 2024, às 12:08:25 (-03:00);
- Observação: Apesar de ocorrer em horário comercial, recomenda-se verificar a legitimidade e conformidade deste acesso;

4.6. Conformidade com a PSI:

4.6.1 As políticas de log e retenção estão em conformidade com a PSI;

4.6.2 Os acessos aos servidores são realizados via conexão segura (*Virtual Private Network* -VPN), garantindo criptografia dos dados transmitidos;

4.6.3 A criação de novos usuários segue boas práticas de gerenciamento de identidades, sendo precedida por solicitações documentadas e aprovadas;

4.7. Vulnerabilidades Identificadas:

4.7.1 O site previdencia.salvador.ba.gov.br, desenvolvido em WordPress, apresenta maior risco devido à sua popularidade como alvo de ataques hackers;

4.7.2 O uso do usuário "root" para acessos administrativos dificulta a rastreabilidade das ações;

5. Recomendações

5.1. Monitoramento Proativo

- Implementar um painel de visualização (dashboard) para monitoramento em tempo real de falhas de acesso e alertas nos sites de uso da DPR;
- Avaliar a possibilidade de compartilhar dashboards de monitoramento já existentes na COGEL, adaptando-os às necessidades da DPR;

5.2. Auditorias Regulares

- Realizar auditorias mensais dos logs de acesso para detecção de atividades anômalas;

5.3. Gestão de Contas e Privilégios

- Reduzir o uso da conta "root" e adotar contas individuais com privilégios

específicos;
- Garantir que todas as atividades administrativas sejam realizadas por contas rastreáveis;

5.4. Atualizações de Segurança

- Priorizar a atualização periódica do WordPress e seus plugins no site previdencia.salvador.ba.gov.br;
- Estabelecer um cronograma de manutenção preventiva para todos os sistemas;

6. Conclusão

A auditoria revelou que os serviços da DPR possuem um sistema robusto para geração e armazenamento de logs, essencial para a segurança e auditoria de TI. No entanto, foram identificadas áreas que necessitam de melhorias, especialmente no monitoramento proativo e na gestão de contas administrativas.

A implementação das recomendações propostas contribuirá para fortalecer a segurança da informação e garantir maior conformidade com a PSI, além de proporcionar maior eficiência na identificação e resolução de problemas.

Salvador, 27 de março de 2025

IVANILDO DE ARAUJO SILVA:79102352591
Assinado de forma digital por IVANILDO DE ARAUJO SILVA:79102352591
Dados: 2025.03.27 15:08:48 -03'00'

IVANILDO DE ARAUJO SILVA
Matrícula n° 3133835
Supervisão Sistêmico de Gestão
NTI/SEMGE