

NORMATIVO Nº 134

Verificação dos Logs de Manutenção no Banco de Dados da Previdência Usiminas



Previdência USIMINAS U	NORMATIVO VERIFICAÇÃO DOS LOGS DE MANUTENÇÃO NO BANCO DE DADOS DA PREVIDÊNCIA USIMINAS	NÚMERO: 134
		DATA APROVAÇÃO INICIAL: 09/09/2015
		REVISÃO: 00
		DATA DA REVISÃO:
		Página 2 de 5

Índice

Capítulo	Página
1. Objetivo	03
2. Área de Aplicação	03
3. Definições e Abreviaturas.....	03
4. Princípios Básicos.....	03
5. Responsabilidades.....	03
6. Procedimentos	03
7. Anexo I	05

47

[Handwritten signatures and initials]

Previdência USIMINAS U	NORMATIVO VERIFICAÇÃO DOS LOGS DE MANUTENÇÃO NO BANCO DE DADOS DA PREVIDÊNCIA USIMINAS	NÚMERO: 134
		DATA APROVAÇÃO INICIAL: 09/09/2015
		REVISÃO: 00
		DATA DA REVISÃO:
		Página 3 de 5

1. Objetivo

Este Normativo tem como objetivo estabelecer os procedimentos de verificação e avaliação do logging de manutenções efetuados no Banco de Dados da **Previdência Usiminas**, visando garantir a segurança dos sistemas e minimizar impactos de vulnerabilidades e incidentes de segurança.

2. Área de Aplicação

Este normativo se aplica à **Área de Tecnologia da Informação da Previdência Usiminas**.

3. Definições e Abreviaturas

3.1. SQL. Linguagem de programação utilizada para manipular informações em bancos de dados.

3.2. Relatório de ações X SSI executadas. Relaciona os procedimentos que foram executados comparados com as SSI executadas.

4. Princípios Básicos

4.1. Gerais

4.1.1. Os procedimentos a serem executados pela **Área de Tecnologia da Informação da Previdência Usiminas** terão exclusivamente o objetivo de extrair as informações do Banco de Dados relacionadas aos atendimentos de SSI's.

5. Responsabilidades

5.1. Área de Tecnologia da Informação

5.1.1. É de responsabilidade da **Área de Tecnologia da Informação**, a elaboração e apresentação do **Relatório de ações X SSI executadas** (Anexo I).

6. Procedimentos

6.1. Área de Tecnologia da Informação

6.1.1. Executar o comando SQL abaixo e preparar o relatório resumo das ações por usuário executadas no Banco de Dados da **Previdência Usiminas**, para fins de auditoria.

```
SELECT DISTINCT(ACTION_NAME), USERNAME, COUNT(*)
FROM DBA_AUDIT_TRAIL
WHERE USERNAME in ('UBX0085B', 'UBX0101B', 'CFT0253B' ) AND
      timestamp>= to_date('dd/mm/aaaa HH:MM:SS', 'dd/mm/yyyy HH24:MI:SS')
GROUP BY (ACTION_NAME, USERNAME)
ORDER BY USERNAME, ACTION_NAME ;
```

Previdência USIMINAS 	NORMATIVO VERIFICAÇÃO DOS LOGS DE MANUTENÇÃO NO BANCO DE DADOS DA PREVIDÊNCIA USIMINAS	NÚMERO: 134
		DATA APROVAÇÃO INICIAL: 09/09/2015
		REVISÃO: 00
		DATA DA REVISÃO:
		Página 4 de 5

6.1.2. Em função das quantidades de ações por usuário apresentadas no relatório resumo, extrair a relação de todos os 'OS_PROCESS', por meio do comando SQL abaixo e selecionar a amostra para análise do ano a ser verificado. A amostra selecionada deve corresponder a no mínimo 5% (cinco por cento) das ocorrências apontadas no relatório (LOGON/LOGOFF).

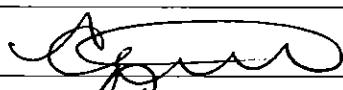
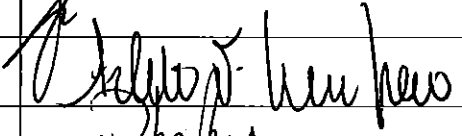
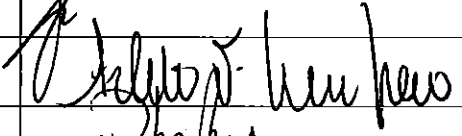
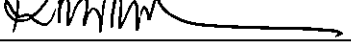
```
SELECT OS_PROCESS FROM DBA_AUDIT_SESSION
WHERE USERNAME IN ('UBX0085B','UBX0101B','CFT0253B' ) AND
TIMESTAMP>= to_date('dd/mm/aaaa HH:MM:SS','dd/mm/yyyy HH24:MI:SS')
ORDER BY OS_PROCESS, EXTENDED_TIMESTAMP;
```

6.1.3. Extrair as ações executando o comando SQL abaixo, inserindo na linha de comando os 'OS_PROCESS' selecionados no item **6.1.2**, para comparação com as SSI executadas, para fins de auditoria.

```
SELECT OS_USERNAME, USERNAME, USERHOST, TERMINAL, TIMESTAMP,
OWNER, OBJ_NAME, ACTION, ACTION_NAME, NEW_OWNER, NEW_NAME,
OBJ_PRIVILEGE, SYS_PRIVILEGE, ADMIN_OPTION, GRANTEE,
AUDIT_OPTION, SES_ACTIONS, LOGOFF_TIME, LOGOFF_LREAD,
LOGOFF_PREAD, LOGOFF_LWRITE, LOGOFF_DLOCK, COMMENT_TEXT,
SESSIONID, ENTRYID, STATEMENTID, RETURNCODE, PRIV_USED,
CLIENT_ID, ECONTEXT_ID, SESSION_CPU,
TO_CHAR(EXTENDED_TIMESTAMP, 'DD-MON-YYYY HH24:MI:SSxFF'),
PROXY_SESSIONID, GLOBAL_UID, INSTANCE_NUMBER, OS_PROCESS,
TRANSACTIONID, SCN, SQL_BIND, SQL_TEXT, OBJ_EDITION_NAME, DBID
FROM DBA_AUDIT_TRAIL
WHERE USERNAME in ('UBX0085B','UBX0101B','CFT0253B' ) AND
timestamp>= to_date('dd/mm/aaaa HH:MM:SS','dd/mm/yyyy HH24:MI:SS') AND
OS_PROCESS in (inserir os 'OS_PROCESS' selecionados).
```

6.1.4. Comparar as evidências da SSI dos procedimentos executados na SSI com o resultado do item **6.1.3**. utilizando os campos 'SQL_TEXT', 'DBID', 'EXTENDED_TIMESTAMP', 'TIMESTAMP', gerando relatório conforme Anexo I.

Este Normativo entra em vigor na data de sua aprovação inicial, devendo ser observada a data da revisão, quando da ocorrência de futuras atualizações processadas no mesmo.

RESPONSÁVEIS		ASSINATURA
ELABORAÇÃO	Celmo de Oliveira	
	João Carlos da Silva Cruz	
CONFERÊNCIA	Humberto Eustáquio Guimarães	
	Rodrigo Picciuti Rodrigues	
APROVAÇÃO	Arleto Faleiro Viegas Greco	
ANUÊNCIA	Rita Rebelo Horta de Assis Fonseca	

Previdência USIMINAS 	NORMATIVO VERIFICAÇÃO DOS LOGS DE MANUTENÇÃO NO BANCO DE DADOS DA PREVIDÊNCIA USIMINAS	NÚMERO: 134
		DATA APROVAÇÃO INICIAL: 09/09/2015
		REVISÃO: 00
		DATA DA REVISÃO:
		Página 5 de 5

Anexo I

Relatório de ações X SSI executadas

SSI :

Evidência das atividades que foram executadas:

OS_PROCESS:

Evidência das ações executadas que foram executadas:

Local e data

Executor da tarefa

Visto do Gestor



