**Número do Parecer:** [0001]

**Data:** 16 de setembro de 2025

**Assunto:** Análise dos Processos de implantação de banco de dados

## 1. IDENTIFICAÇÃO DO SOLICITANTE E DO AVALIADOR

**Solicitante(s):** AUDIN

**Avaliador(es):** Thiago Fernandes da Silva Oliveira.

## 2. LEVANTAMENTO

Este parecer técnico tem por objetivo levantar e analisar os atuais processos de implantação de banco de dados.

Foram identificados os seguintes documentos que tratam do assunto:

- Manual De Normas e Procedimentos De Segurança Da Informação
- Manual De Normas e Procedimentos De Segurança Da Informação - Controle De Acesso Normas De Backup e Recuperação De Dados
- Manual De Normas e Procedimentos Da Gestão De Mudança

Além disso foram feitas entrevistas com atores da SUSIS, SUGOT/GEMUL, NUSIF e SUPRO/GEINS.

### 2.1. MANUAL DE NORMAS E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Foi analisada a versão de 16.1 de 21/02/2024. No capítulo “CAPÍTULO XV - NORMAS E PROCEDIMENTOS DE BACKUP (DADOS E VOZ) E DE ACESSO A BANCO DE DADOS” constam os seguintes processos:

- 18. SOLICITAÇÃO DE EXECUÇÃO DE SCRIPT
- 19. AUTORIZAÇÃO PARA EXECUÇÃO DE SCRIPT
- 20. SOLICITAÇÃO DE ACESSO À BASE DE DADOS DE PRODUÇÃO
- 21. CRIAÇÃO DE LOGINS E ACESSO À BASE DE DADOS DE PRODUÇÃO
- 22. PERMISSÕES DE ACESSO A BASE DOS SISTEMAS DE APLICAÇÃO

Os processos ocorrem através de preenchimento de documentos de solicitação conforme anexos no manual e os scripts devem ser armazenados no repositório de SVN. São estabelecidos processos de autorização para execução de script envolvendo gestores responsáveis do sistema (técnicos e de negócio) de acordo com o teor da mudança, além de uma série de normas a serem obedecidas no processo como template de script a ser obedecido, passar pelo processo de mudança antes da execução de DDL, etc.

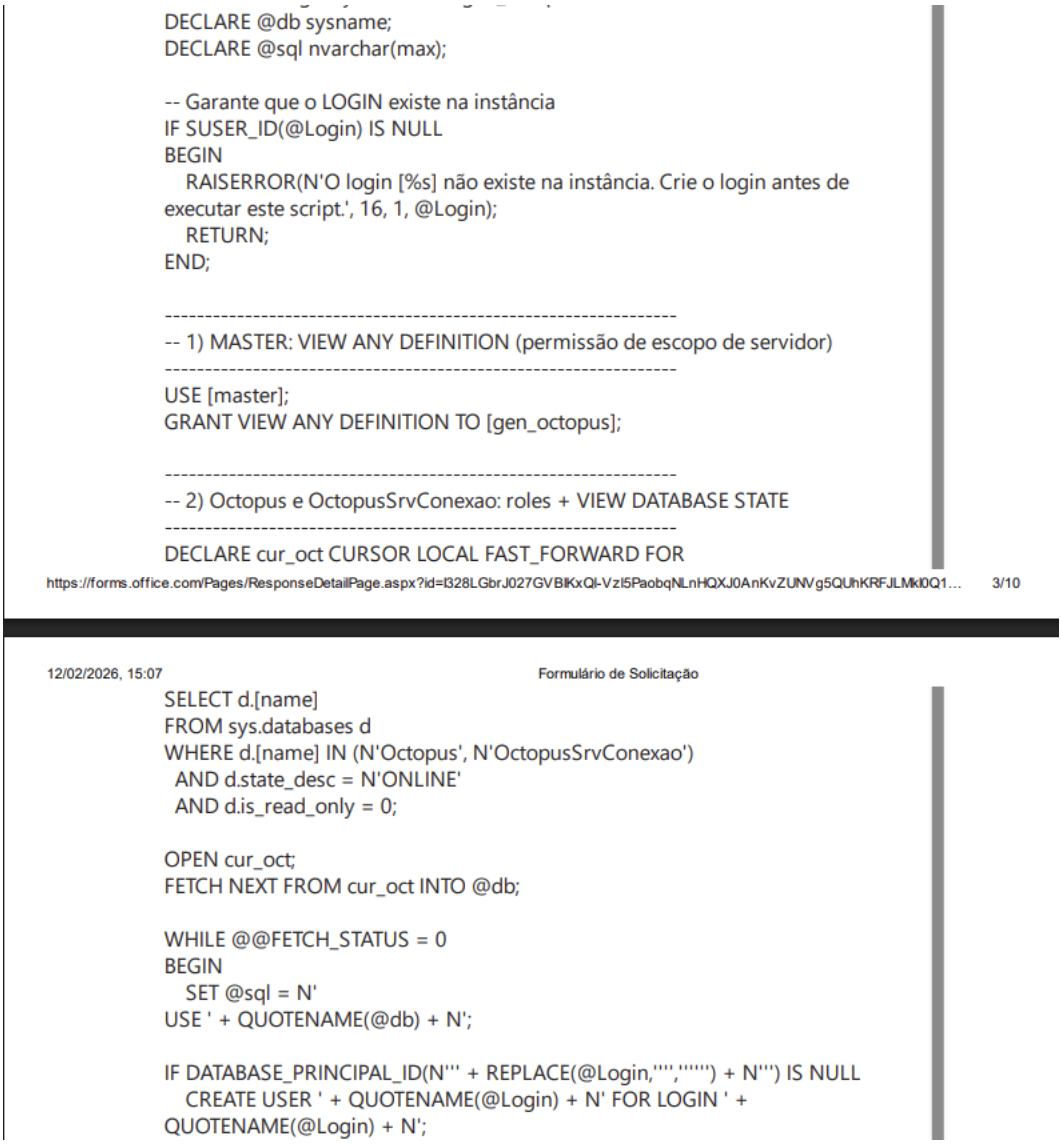
### 2.2. MANUAL DE NORMAS E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO - CONTROLE DE ACESSO NORMAS DE BACKUP E RECUPERAÇÃO DE DADOS

Sessões relacionadas:

- CAPÍTULO I – Gestão e Controle De Acesso - 6.2.Normas Gerais De Controle De Acesso
- CAPÍTULO II: Backup E Recuperação De Dados - 20. SOLICITAÇÃO DE EXECUÇÃO DE SCRIPT” e 21. Autorização Para Execução De Script

As regras definem um processo através do uso de SVN para armazenar arquivos e de um formulário como documentação formal para solicitações.
O formulário está disponível em Formulário de Solicitação via *Forms do Office*.

Figura 1. Formulário de Solicitação de Execução de Script



```
DECLARE @db sysname;
DECLARE @sql nvarchar(max);

-- Garante que o LOGIN existe na instância
IF SUSER_ID(@Login) IS NULL
BEGIN
   RAISERROR(N'O login [%s] não existe na instância. Crie o login antes de
executar este script.', 16, 1, @Login);
   RETURN;
END;

-------------------------------------------------------------
-- 1) MASTER: VIEW ANY DEFINITION (permissão de escopo de servidor)
-------------------------------------------------------------
USE [master];
GRANT VIEW ANY DEFINITION TO [gen_octopus];

-------------------------------------------------------------
-- 2) Octopus e OctopusSrvConexao: roles + VIEW DATABASE STATE
-------------------------------------------------------------
DECLARE cur_oct CURSOR LOCAL FAST_FORWARD FOR
```





```
SELECT d.[name]
FROM sys.databases d
WHERE d.[name] IN (N'Octopus', N'OctopusSrvConexao')
  AND d.state_desc = N'ONLINE'
  AND d.is_read_only = 0;

OPEN cur_oct;
FETCH NEXT FROM cur_oct INTO @db;

WHILE @@FETCH_STATUS = 0
BEGIN
   SET @sql = N'
USE ' + QUOTENAME(@db) + N';

IF DATABASE_PRINCIPAL_ID(N''' + REPLACE(@Login,'''',''''') + N''') IS NULL
   CREATE USER ' + QUOTENAME(@Login) + N' FOR LOGIN ' +
QUOTENAME(@Login) + N';
```

Figura 2. Formulário de Solicitação de Execução de Script Impresso em PDF

## 2.3. MANUAL DE NORMAS E PROCEDIMENTOS DA GESTÃO DE MUDANÇA

O Manual estabelece o processo de mudança que deve ser usado para scripts de DDL (*Domain Definition Language*) e que deve ser anexado a documentação formal conforme regulamento interno (Segurança, Mudança, Outros).

## 2.4. Entrevistas

Nas entrevistas fizemos as seguintes descobertas:

- Estão sendo aceitas as duas abordagens de documentação formal (formulário e documento);
- Os scripts são gerados pelos fornecedores e pela equipe interna de desenvolvimento, porém os fornecedores não possuem acesso ao formulário e um analista do banco precisa copiar de um documento para o formulário;
- O formulário está sendo impresso como PDF após o preenchimento;
- O formulário precisa de uma assinatura (foi relatado uso da assinatura digital);

- Foi relatada ideia de automatizar a criação de registro de mudança ou chamado a partir do formulário, ou de uso de formulário através da ferramenta de service desk;
- No caso do formulário o script vem junto com formulário, e acaba vindo cortado entre as páginas dificultando a execução e análise no processo de mudança.

## 3. ALINHAMENTO COM PROCESSOS DE MERCADO

Fizemos uma pesquisa relacionando os processos com normativos internacionais (ISO 27001, ITIL v4, COBIT 2019) e apresentando soluções estruturadas para cada item. O objetivo é elevar o nível de maturidade do processo de gerenciamento de scripts DDL em ambientes de produção, alinhando-o com as melhores práticas e exigências regulatórias. Com base na pesquisa identificamos alguns gaps nos processos.

### 3.1. Falta de SLA Explícito em Mudanças de Banco de Dados

O manual de gestão de mudança  faz referência aos dias de implantação e número máximo de RDMs a serem executadas, mas não existem SLAs previstos para execuções de mudanças.

**Referência Normativa**:

- ISO 27001:2022: Deve-se documentar e comunicar políticas que incluam cronogramas, prioridades e aprovações de mudanças
- ITIL v4: Mudanças devem ser priorizadas e agendadas conforme tipo e impacto; SLAs devem ser definidos por categoria de mudança
- COBIT 2019: Categorizar mudanças (standard, normal, emergency) e aplicar cronogramas diferentes conforme categoria

### 3.2. Falta de Matriz de Risco Específica para Scripts DDL

O processo atual avalia risco via formulário genérico de risco, através de análise via CCM e classificação do tipo de RDM. Não existe matriz diferenciada entre scripts CREATE TABLE / DROP TABLE / ALTER INDEX, etc, mesmo que um DROP seja inerentemente mais arriscado que um CREATE.

**Referência Normativa**:

- ISO 27001:2022: A organização deve determinar e analisar os riscos [...] relacionados à introdução, mudança ou retirada de controles. Mudanças em sistemas de informação [...] devem ser controladas e avaliadas conforme o risco potencial
- ITIL v4: Mudanças devem ser categorizadas por tipo (patch, config, release, emergency) e risco; risco varia conforme impacto técnico
- COBIT 2019: Categorizar mudanças e usar critérios específicos de priorização (business need, technical risk, compliance impact)

### 3.3. Ausência de Cadeia de Custódia e Rastreabilidade Forte em Scripts

O processo atual documenta scripts via SVN, anexo de formulário na RDM, aprovação registrada no ITSM, conformidade manual pela GEMUL. Não existe rastreabilidade entre versão do script no SVN e script executado em produção, correlação entre RDM e uma aprovação do analista no repositório de versão (SVN), validação automática de nomenclatura conforme Manual de Padrão de nomenclatura de banco de dados, rastreio de quem acessou/modificou o script entre aprovação e execução.

**Referência Normativa**:

- ISO 27001:2022: Manter registros evidenciando autorização, aprovação, execução e revisão de mudanças; trilha de auditoria deve ser completa e não-repudiável. Mudanças [...] devem ser implementadas sob controle de forma a garantir que nenhuma mudança nao-autorizada seja introduzida.
- ITIL v4: Documentação de mudanças deve incluir: quem solicitou, quem aprovou, quando foi implementado, resultado da implementação. Retenção de registros por período definido.
- COBIT 2019: Mudanças devem incluir versão de código, dependências, e trilha de implementação (from request to deployment)

### 3.4. Ausência de Automatização em Nomenclatura de Scripts

O MNP de Gestão de Mudança estabelece regras rígidas de nomenclatura, sequencial, fornecedor, base de dados, tipo de objeto, descrição do objeto. A validação é manual pelos analistas da GEMUL.

**Referência Normativa**:

- ISO 27001:2022: mudanças devem ser implementadas sob controle formalmente definido.
- COBIT 2019: Impacto de mudanças deve ser avaliado sistematicamente, incluindo conformidade com padrões

## 4. ANÁLISE SOBRE PROCESSOS

Considerando tudo que foi levantado chegamos as seguintes conclusões:

- A existência de dois manuais tratando do mesmo assunto provoca ambiguidade e dúvida sobre qual abordagem adotar;
- O manual que fala sobre o uso do formulário define a necessidade do uso da SVN para guardar os scripts, porém o formulário possui um campo para preencher o script ao invés de link da SVN;
- O requisito do formulário ser assinado não está presente no manual;
- A falta de permissão dos fornecedores para preencher o formulário pode provocar erro humano no momento de copiar script de um documento;
- O formulário facilita o processo de auditoria de mudanças;

## 5. RECOMENDAÇÕES

- Revogar um dos manuais sobre a documentação formal ou atualizar removendo o conflito de definições;
- Repensar o uso do formulário via office como estratégia de registro, alterar para formulário direto na ferramenta de service desk;
- Alterar forma de guardar os scripts para uso do repositório de código Git ao invés da SVN, avaliando se ficaria junto com a aplicação ou repositório apartado;
- Repensar o processo de armazenamento de scripts para evitar retrabalho de copiar scripts de local para outro, manter em um local único, com acesso do fornecedor e acessível por ferramentas que permitam automatização (liquibase, flyway);

- Automatizar o processo de criação de banco de dados, de usuário, de alteração de permissões com aprovação manual pela(s) áreas que forem necessárias.
- Definir SLAs para mudanças de banco de dados por tipo de mudança e criticidade, ex.: Normal/Baixa 5 dias úteis, Normal/Média 3 dias úteis, Emergencial 1 hora.
- Classificação de Scripts DDL por Risco Técnico.
- Implementar pipeline gitops com validação automática e rastreabilidade forte.