PODER JUDICIÁRIO DO ESTADO DO ACRE

Tribunal de Justiça

MANUAL DE PROCEDIMENTOS

DIRETORIA: DIRETORIA DE DE TECNOLOGIA E INFORMAÇÃO

UNIDADE: GERÊNCIA DE BANCO DE DADOS E SEGURANÇA DA INFORMAÇÃO

NOME DO PROCESSO: GERENCIAR BANCO DE DADOS E SEGURANÇA

CÓDIGO: MAP-DITEC-002 VERSÃO: 01

PODER JUDICIÁRIO
DO ESTADO DO ACRE

Rio Branco - Acre

SUMÁRIO

1 OBJETIVO

Estabelecer os procedimentos para o gerenciamento dos bancos de dados do TJAC.

2 DOCUMENTAÇÃO NORMATIVA DE REFERÊNCIA

- Resolução do Tribunal Pleno Administrativo nº 237/2019.
- Resolução do Tribunal Pleno Administrativo nº 180/2013.
- Resolução do Tribunal Pleno Administrativo nº 166/2012.

3 ORIENTAÇÕES GERAIS

- As solicitações de atendimento relacionados às demandas de TI devem ser realizadas exclusivamente através de abertura de chamado por meio da plataforma GLPI (https://glpi.tjac.jus.br/), instituído como meio de comunicação interna com a DITEC, registrando os incidentes e requisições, conforme previsto na Resolução nº 29 de 27 de janeiro de 2017;
- Tutorial para abertura de chamados: https://www.youtube.com/embed/wurddK4JIsY
- Os pedidos de *logins* devem ser feitos pela Diretoria de Pessoas - DIPES, conforme art. 44, *caput,* da Resolução Nº 226/2018, através de solicitação aberta no sistema de chamados GLPI, na categoria “usuário de rede > Acesso para novo usuário servidor ou comissionado (e-mail, pandion, computador, wifi, glpi) ”, encaminhado à GESEG, e deve conter os seguintes dados:
  - nome completo;
  - matrícula;
  - CPF;
  - Cargo/Função;
  - Setor/Órgão.

- Os *logins* somente são bloqueados e inativados pelos seguintes motivos: solicitação formal do gestor da unidade, exoneração, demissão ou aposentadoria do funcionário;
- Os *logins* são bloqueados temporariamente pelas seguintes razões: afastamento do funcionário, a pedido da chefia imediata do mesmo, segurança, mau uso ou uso suspeito;
- Os servidores que tiveram seus *logins* bloqueados e, por qualquer motivo, queiram voltar a utilizá-los, devem solicitar a seus respectivos chefes de setores para abrir uma solicitação por meio do sistema de chamados GLPI;
- Caso não haja solicitação direta da DIPES, o chamado deverá ser aberto com os dados já informados, ficando o solicitante responsável pelo cadastro realizado fora da regra padrão.

4 DESCRIÇÃO DAS ATIVIDADES

4.1 GESTÃO DOS BANCOS DE DADOS

- A Gerência de Banco de Dados – GEBAN, recebe da Gerência de Sistemas – GESIS as necessidades de objetos e usuários dos bancos de dados solicitadas pelos analistas de desenvolvimento, através do sistema GLPI;
- Quantifica o espaço a ser ocupado no banco de dados pelos objetos e usuários;
- Cria o espaço físico a ser ocupado pelos objetos de banco de dados no servidor;
- Disponibiliza o espaço à Gerência de Sistemas para o acesso aos objetos de banco de dados;
- Cria o usuário de banco de dados com direito de criação de objetos no espaço físico destinado a ele;
- Concede as permissões internas do banco de dados a este novo usuário;
- Verifica periodicamente os seguintes aspectos:
  - Disponibilidade dos Bancos de dados e Servidores de Aplicação;
  - Quantidade de usuários conectados e ativos;
  - Conexões alheias aos sistemas;
  - Transações longas consumindo recursos operacionais em excesso;
  - Alocação de espaço livre nas diversas *tablespaces* e *file systems*;
  - Conexões com outras instâncias;
  - Integridade dos objetos replicados de outras instâncias; e
  - Existência de objetos inválidos.
- Registra as informações sobre o desempenho dos bancos de dados nos sistemas gerenciadores de bancos de dados; e
- Observa o crescimento dos bancos de dados e avalia a possibilidade de substituição, particionamento e outras ações destinadas a garantir a segurança dos dados.

4.2 *BACKUP* E *RESTORE* DOS DADOS

- Gerência de Segurança da Informação analisa as informações contidas nos servidores de domínio, servidores de aplicações, servidores de arquivos e servidores de sistemas corporativos e identifica a plataforma de hardware, o sistema operacional do servidor, o meio de armazenamento externo disponível para aquele servidor e o software do banco de dados ali instalado;
- Estima a quantidade de objetos de banco e sua adequação ao limite de espaço do meio de armazenamento;
- Escreve *script* de teste para mensurar tempo de execução;
- Define a periodicidade de execução (diário, semanal e mensal) do backup ou restore, procurando o melhor horário e períodos para execução do procedimento e a forma de realização (manual ou automático);
- Define o prazo de retenção dos *backups*, com base nas informações contidas nos servidores de domínio, servidores de aplicações, servidores de arquivos e servidores de sistemas corporativos;
- Registra no formulário “Informações para Backup e Restore” (FOR-DITEC-002-01) as informações de nome do servidor, periodicidade de execução, horário de execução, forma de realização, prazo de retenção;
- Periodicamente acompanha as execuções, medindo tempos de execução e a quantidade de dados que está sendo copiada;
- Particiona, de acordo com os tempos e quantidade de dados medidos, as execuções do procedimento de *backup* ou de *restore* para horários diferentes, separando ou dualizando a gravação em máquinas diferentes;
- Inicia os procedimentos de *backup* ou *restore*, conforme o caso;
- Monitora a execução dos procedimentos;
- Verifica presença de falhas, interrupções e insucessos, e registra no formulário “Erros em Procedimentos de Backup” (FOR-DITEC-002-02);
- Procura a solução para as ocorrências e registra a solução no formulário “Erros em Procedimentos de Backup” (FOR-DITEC-002-02); e

- Arquivar os *backups* executados nos *storages*, unidade de fita e em outro ambiente físico, em meios equivalentes ao sítio principal.

4.3 SOLICITAÇÃO DE ACESSO DE USUÁRIO AOS SERVIÇOS DE TI

- A Gerência de Banco de Dados e Segurança (GEBAN) recebe das unidades organizacionais do TJAC as Solicitação de Acessos de Usuários aos Serviços de TI, através do GLPI;
- O chamado pode conter solicitação relacionada à criação de novo usuário com inclusão de serviços relacionados a acesso, à rede corporativa, internet, correio eletrônico, mensagem instantânea ou alteração de acesso, bloqueio ou desbloqueio;
- Sempre que um novo servidor (efetivo ou *ad nutum*) é admitido, a DIPES abre chamado através do GLPI e encaminha para a Gerência de Redes e Segurança para criação do login do novo usuário e a concessão dos permissionamentos;
- Sempre que um servidor (efetivo ou ad nutum) for exonerado, a DIPES abre um GLPI e encaminha para a GESEG, para bloqueio do login do usuário e posterior exclusão;
- GESEG providencia as alterações solicitadas acessando o Active Directory (AD).
- Para a criação dos *logins* dos usuários, a GESEG toma as seguintes providências:
  - Verifica no chamado o nome completo do usuário;
  - Separa o nome e o último sobrenome, e consulta no Active Directory (AD) a existência de usuário com o mesmo *login*;
  - Compõe o *login* do usuário da seguinte forma: nome.sobrenome, conforme exemplo a seguir:
    - Usuário: Alberto Nunes da Silva → *Login*: alberto.silva
  - No caso de já existir usuário com o mesmo *login*, compõe o *login* do usuário com o nome e o antepenúltimo sobrenome, caso exista, conforme exemplo a seguir:
    - Usuário: José Cordeiro dos Santos → *Login*: jose.cordeiro
  - Os usuários com nomes compostos devem ter seu *login* com o nome composto e o sobrenome, conforme exemplo a seguir:

- Usuário: João Marcelo Santana Ramos → *Login*: joaomarcelo.ramos

- A criação do endereço de correio eletrônico segue a mesma regra de criação do *login* dos usuários;
- O correio eletrônico das unidades organizacionais deve seguir as siglas das unidades organizacionais definidas no Siglário do Poder Judiciário;
- A solicitação de endereço de correio eletrônico pelas unidades organizacionais é realizada por meio de abertura de chamado no GLPI, onde o gestor da unidade informa os endereços desejados e os usuários que podem acessá-lo;
- Sempre que houver alteração no *login* ou nas permissões de acesso do usuário, a GESEG informa o solicitante e fornece orientação sobre o cadastramento de senha.

4.4 CONTROLE DE PROGRAMAS MALICIOSOS

- Para manter todos os computadores do TJAC com o antivírus instalado e atualizado, a Gerência de Segurança realiza as seguintes tarefas:
  - Analisa os relatórios emitidos pelo *software* antivírus, a fim de detectar computadores com o antivírus desatualizado ou não instalado;
  - Tenta instalar ou atualizar remotamente o antivírus nos computadores detectados pelo processo acima;
  - Caso não seja possível realizar o procedimento remotamente, solicita apoio da Diretoria Regional responsável pela unidade para proceder à instalação e/ou a atualização do antivírus no local;
  - Mantêm-se informado sobre o surgimento de novas ameaças, melhores práticas e novos produtos;
- Ao tomar conhecimento do surgimento de novas ameaças, a GESEG realiza as seguintes tarefas:
  - Identifica o modo de operação da ameaça;
  - Toma as providências cabíveis para que o ambiente computacional do PJAC esteja o mais protegido possível contra essa ameaça; e
  - Analisa os relatórios e alertas de infecção emitidos pelo *software* antivírus durante todo o dia, procurando por sistemas infectados.
- No caso de encontrar um sistema infectado:
  - Identifica o(s) computador(es) afetado(s);
  - Identifica qual(is) programa(s) malicioso(s) está(ão) agindo no sistema;
  - Verifica qual a forma de desinfecção e proteção contra futuras infecções; e
  - Orienta a Diretoria Regional sobre como proceder à desinfecção.
- Realiza varreduras constantes na rede em busca de programas maliciosos instalados;

- Para manter os servidores de antivírus atualizados, e em perfeito funcionamento, a GESEG executa as seguintes tarefas:
  - Monitora constantemente o uso dos recursos dos servidores, a fim de detectar a necessidade de ajustes e/ou *upgrade* dos mesmos;
  - Mantêm-se informado sobre o lançamento de novas versões do *software* antivírus;
  - Aplica o mais breve possível as atualizações disponibilizadas pelo fabricante do *software* antivírus;
  - Realiza o *backup* da base de dados dos servidores de antivírus;
  - Mantêm o antivírus do servidor de correio eletrônico atualizado; e
  - Bloqueia arquivos anexados às mensagens de correio que potencialmente possam conter programas maliciosos, de acordo com a política adotada pela DITEC.
- Procedimento para desbloqueio de arquivos anexados às mensagens de correio eletrônico:
  - Recebe a solicitação de desbloqueio feita pelo usuário, através do GLPI;
  - A solicitação deve conter o número de identificação do anexo bloqueado, a data de recebimento da mensagem e o endereço de correio eletrônico do usuário que recebeu a mensagem;
  - Localiza o anexo bloqueado no servidor de correio eletrônico;
  - Verifica a confiabilidade do arquivo bloqueado e a presença de programas maliciosos no mesmo;
  - Libera ou não o anexo bloqueado, de acordo com o resultado da verificação;
  - Informa ao usuário sobre a liberação ou não do anexo e, em caso de liberação, informa também a localização do anexo desbloqueado; e
  - O anexo desbloqueado fica disponível para o usuário por um período de dias predeterminado, sendo depois excluído do servidor.
- Orienta os usuários, quando solicitado através de GLPI, quanto às suspeitas e dúvidas a respeito de infecção por programas maliciosos.

4.5 DISTRIBUIÇÃO DE ATUALIZAÇÕES CRÍTICAS DE SEGURANÇA

- Para manter os microcomputadores do ambiente computacional do PJAC com os sistemas atualizados com relação à segurança, a Gerência de Segurança executa as seguintes tarefas:
  - Mantêm-se informada sobre o lançamento de atualizações críticas de segurança para os sistemas utilizados no ambiente computacional do PJAC;
  - Efetua o *download* das atualizações em local apropriado;
  - Realiza estudos e testes para que a atualização dos sistemas cause o menor impacto possível no ambiente de produção do PJAC;
  - Executa varreduras constantes na rede de computadores do TJAC, a fim de identificar sistemas desatualizados;
  - Promove a instalação das atualizações críticas através do servidor e do *software* de distribuição de *softwares*; e
  - Solicita apoio da Diretoria Regional quando a instalação remota não tiver sido bem sucedida.

4.6 CONTROLE DE SPAM

- Para manter controlado o número de mensagens indesejadas (SPAM) em circulação na rede de computadores do PJAC, a Gerência de Segurança realiza as seguintes tarefas:
  - Monitora e mantêm o(s) servidor(es) anti-spam em perfeito funcionamento; e
  - Otimiza e aplica as regras de bloqueio de mensagens indesejadas.
- Analisa os relatórios emitidos pelo *software* anti-spam, a fim de garantir que o maior número de mensagens indesejadas e o menor número de mensagens legítimas sejam bloqueados.

5 GESTÃO DO PROCESSO

- A Gerência de Banco de Dados (GEBAN) acompanha regularmente os indicadores para verificar tendências nas demandas e possibilitar o gerenciamento da equipe;
- Realiza, a cada seis meses, Reunião de Equipe (RE) para discutir questões relacionadas à melhoria e à gestão do processo;
- A RE é documentada para evidenciar a análise dos processos.

6 INDICADORES

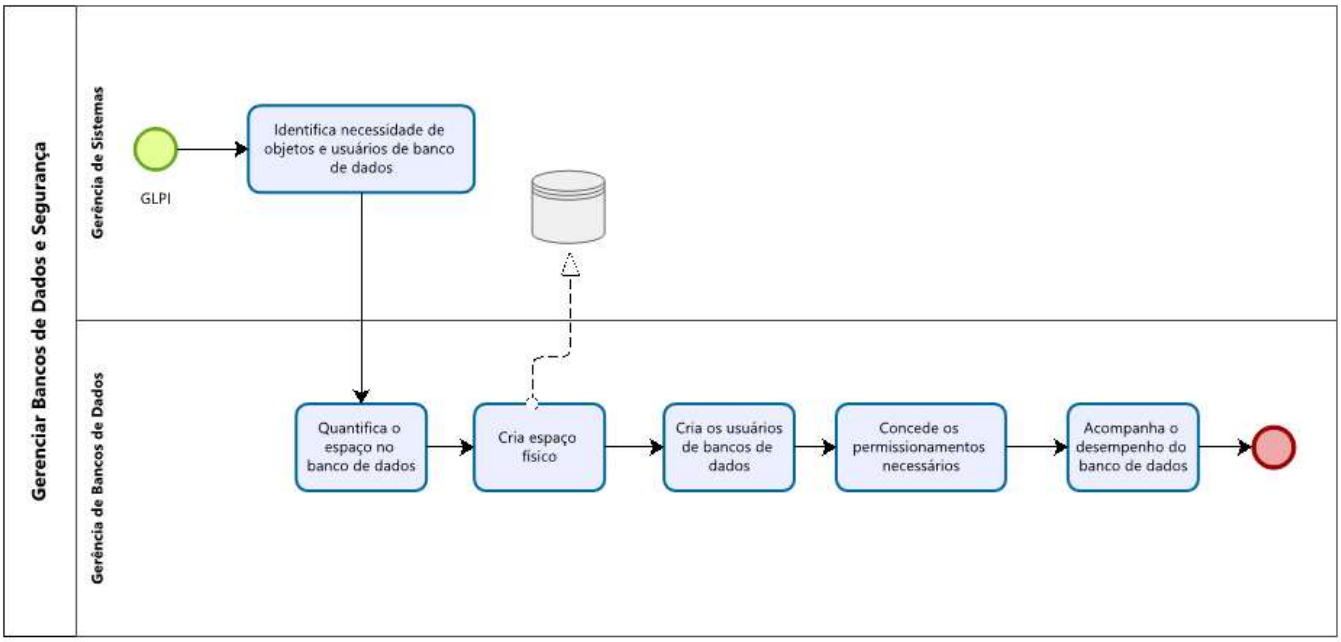
Nome	Fórmula	Meta	Período de apuração	Fonte
Demanda	Solicitação de Serviços de TI recebidas		Mensal	FOR-DITEC-002-04

7 REGISTROS

Identificação	Armazenamento	Tempo de Guarda	Destinação
Informações para *backup* e *restore* (FOR-DITEC-002-01)	Pasta eletrônica	2 anos	Eliminação
Registro de falhas em procedimentos de *backup* e *restore* (FOR-DITEC-002-02)	Pasta eletrônica	2 anos	Eliminação
Solicitação de acessos de usuários aos serviços de TI	GLPI	1 ano	Eliminação

8 ANEXOS

- Anexo 1: Fluxograma do processo de gerenciamento de bancos de dados;



- Anexo 2: Gerir certificado digital