Laboratório de Sistemas Integráveis Tecnológico

PROJETO SREI

Sistema de Registro Eletrônico Imobiliário

PA2.7.2 - Procedimentos operacionais de T.I.

Sumário

1 Introdução

Este documento descreve o conjunto mínimo de procedimentos operacionais de T.I. necessários para suportar de forma segura e confiável a operação dos sistemas SREI.

A não aplicação ou falhas na implementação dos seguintes procedimentos podem gerar graves prejuízos às operações de T.I. do cartório, podendo gerar perdas ou comprometer a integridades dos dados de registros.

2 Procedimentos operacionais de T.I.

A seguir são relacionados os procedimentos operacionais mínimos a serem cumpridos a fim garantir a segurança e a integridade dos dados de registros SREI:

- Procedimento de backup;
- Procedimento de gerenciamento de mudanças;
- Procedimento de gerenciamento de patches;
- Procedimento de sincronismo de relógios;
- Controle contra códigos maliciosos.

3 Procedimento de backup

3.1 Objetivo

O objetivo da geração de cópias de segurança consiste em manter a integridade e a disponibilidade da informação e dos recursos de processamento de informação, principalmente, aqueles que consistem na operação do SREI. Assim

3.2 Responsabilidades

Todos os usuários têm responsabilidades individuais pelas cópias de segurança, as quais DEVEM ser identificadas em seus acordos de utilização.

Todas as entidades envolvidas na operação do SREI são responsáveis por assegurar que os dispositivos de backup e as instruções de trabalho estejam em conformidade com os requisitos gerais aplicáveis definidos no documento de requisitos gerais do SREI.

Cada entidade é responsável por assegurar que a equipe de TI execute os backups identificados conforme necessário e ainda identifique e relate todos os possíveis defeitos, falhas ou erros.

O Suporte é responsável por documentar, testar e manter o processo de restauração de acordo com os requisitos.

3.3 Realização do backup

3.3.1 Definição do escopo de backup

Todos os itens inclusos na realização do backup devem ser formalmente documentados dentro de um escopo.

Este escopo deve conter todos os sistemas contemplados e os respectivos dados que devem possuir salvaguarda.

TODOS os dados relativos aos proprietários de direito e outras informações criticas para a operação do SREI devem estar inclusos.

3.3.2 Periodicidade do backup

Os backups devem ser realizados a intervalos DIARIOS de forma INCREMENTAL.

3.3.3 Realização

Preferencialmente, o backup deve ser realizado de forma automatizada por ferramenta. Todos os horários de realização de backup devem ser documentados junto ao escopo.

Os backups automatizados devem ser programados para serem realizados durante o período de menor atividade da entidade.

A ferramenta de automatização de backups deve verificar a integridade e condições de restauração dos backups logo após sua realização.

Caso, por inviabilidade operacional, os backups não possam ser realizados de forma automática por ferramenta, estes devem ser realizados sob as mesmas condições, porem com o acompanhamento de um colaborador responsável.

As funções deste colaborador para a realização dos backups também devem estar documentadas.

3.3.4 Registros de backup

Registros de backup devem ser gerados de forma automática após a geração de cada backup.

Estes registros devem conter TODOS os itens copiados e, também, a hierarquia exata entre os diretórios copiados.

Estes registros devem ser verificados manualmente em contrapartida aos dados originais.

Estes registros devem ser mantidos de forma organizada e considerados arquivos confidenciais.

3.3.5 Verificação de integridade de conteúdo do backup

A verificação de integridade do conteúdo dos backups realizados somente pode ser realizada através de ferramenta automatizada.

Esta verificação deve ocorrer através da própria ferramenta que gerou os backups ou através de ferramenta terceirizada aprovada e documentada pela entidade.

Manualmente, devem ser verificadas as condições dos atributos de acesso do conteúdo. Para isso, o seguinte procedimento deve ser realizado:

- Realizar a copia de uma amostra de arquivos, através dos procedimentos utilizados normalmente;
- Realizar teste de comparação através da visualização das propriedades dos arquivos originais e das copias;
- Os atributos devem estar impreterivelmente, identicos.

3.4 Salvaguarda dos backups

3.4.1 Backups lógicos

O Servidor que armazena os dados de backup deve estar alocado em área de segurança de nível 3.

Somente os colaboradores autorizados devem possuir acesso a estes servidores.

Os discos de armazenamento destes servidores devem estar configurados em redundância (RAID 1 ou RAID 5).

3.4.2 Copias em mídias físicas

As copias em mídias físicas devem ser realizadas somente em medias homologadas para fins de backup.

Todo manuseio e transporte destas mídias devem ser realizado por colaborador autorizado. Esta autorização deve estar documentada.

As mídias devem ser armazenadas em local especifico obedecendo as especificações dos fabricantes (ver 4.5).

As condições das mídias físicas devem ser testadas a intervalos anuais, visando à integridade e funcionalidade completa das mídias.

3.5 Restauração do backup

3.5.1 Teste de Restauração

O processo de restauração deve ser testado mensalmente visando às condições de restauro das mídias e a abrangência e eficiência do processo.

Os testes devem ser realizados através da restauração de uma amostra de backups em servidores de teste e homologação.

Deve ser garantido que todos os itens documentados da amostra de backup utilizada sejam restaurado com sucesso, incluindo seus atributos.

3.5.2 Restauração do backup

A restauração deve ocorrer sempre quando do acontecimento de um incidente de segurança que afete a integridade dos dados de produção.

A restauração deve ser realizada através de ferramenta automatizada ou através do próprio software de banco de dados, quando viável.

Todo o processo de restauração deve ser acompanhado por colaborador responsável.

Após restauração, todo o conteúdo deve ser verificado através da verificação dos registros gerados quando da geração das copias de segurança.

4 Procedimento de gestão de mudanças

4.1 Objetivo

Descrever e suportar o processo de gerenciamento de mudanças para alterações no ambiente de T.I.

4.2 Escopo e Aplicação

O presente procedimento se aplica a todas áreas de tecnologia da Informação do ambiente SREI que necessitam realizar qualquer mudança na configuração do ambiente ou dos seus componentes. São assim incluídos no escopo do presente procedimento a instalação, a atualização e a substituição de qualquer sistemas de hardware ou software. Ainda são escopo do procedimento quaisquer alterações na configuração do ambiente de T.I., alterações na configuração dos sistemas de hardware e software.

É excluído da aplicação do presente procedimento o processo de gerenciamento de pacthes, pelo qual DEVE ser utilizado o especifico procedimento.

4.3 Procedimento operacional

Qualquer mudança em sistemas de T.I. DEVE ser planejada, aprovada, testada e documentada de forma apropriada à complexidade e à sensibilidade dos sistemas afetados.

No mínimo o procedimento de gestão de mudança DEVE incluir os procedimentos descritos a seguir.

4.3.1 Registro

DEVE ser mantido um registro completo de todas as mudanças realizadas contendo os seguintes elementos:

- Descrição das alterações, configurações, instalações e atualizações realizadas;

- Nome dos responsáveis e dos executores da correção;
- Data;
- Propósito;
- Qualquer observação feita durante a mudança.

4.3.2 Plano de implementação

Os responsáveis da área de T.I. devem preparar o plano de implementação detalhando as soluções técnicas definidas, o cronograma e os plano de teste e de roll back.

O plano de implementação detalha todos os estágios que são requeridos para gerenciar as alterações com sucesso, isso inclui o plano de testes e a estratégia de "Roll back". Para alterações mais complexas pode também ser incluída uma agenda e o cronograma do projeto.

Para mudanças críticas que implicam em modificações significativas é recomendado que a mudança seja previamente testada e avaliada em ambiente de homologação.

4.3.3 Avaliação de risco

Sucessivamente o plano de implementação DEVE ser aprovado pelos responsáveis de cada área de negocio afetada pela mudança.

DEVEM assim ser levantadas junto com as partes interessadas todos os sistemas e processos afetados pela alteração proposta e listar todos os impactos e os relativos riscos identificados. A Avaliação de Risco é utilizada para criar a recomendação de mudança, garantindo que os riscos para o negócio tinham sido identificados e tratados.

4.3.4 Efetivação da mudança

O responsável de T.I. DEVE dar inicio ao processo na data e horário que possuir o menor efeito possível nos serviços e DEVE acompanhar o processo de mudança ate o final verificando que o plano seja executado conforme a especificação.

O responsável de TI antes de dar inicio ao processo de mudança deve verificar que todos os requisitos de pessoal e projeto estejam atendidos.

Ele é também responsável por decidir o adiamento ou cancelamento do processo caso algum requisito não seja atendido. Em caso de adiamento as partes envolvidas são interpeladas para definir o novo planejamento

4.3.5 Revisão Pós-Implementação

Ao final da implementação DEVEM ser aplicados os procedimentos definidos para validar a efetividade da mudança e para detectar eventuais problemas consequentes das operações realizadas.

Caso não seja possível resolver os problemas detectados na janela de tempo definida DEVE ser disparado o procedimento de Roll Back.

4.3.6 Procedimento de Roll Back

O procedimento de Roll Back deve restaurar o ambiente na configuração anterior ao procedimento de mudança.

Desta forma todas as alterações, instalações e configurações realizadas durante o processo de mudança DEVEM ser desfeitas de forma a restaurar o estado anterior.

Devido a dificuldade de restaurar o estado anterior é muito importante que cada procedimento aplicado durante a mudança tinha sido documentado durante a sua execução de forma que o processo de Roll Back possa ser executado com o maior nível de sucesso possível.

Em caso de necessidade de Roll Back, a ultima versão da cópia de segurança poderá ser utilizadas para a restauração do sistema.

4.3.7 Cópias de segurança

Antes de realizar qualquer operação de mudança DEVE ser realizada uma copia de segurança do ambiente.

Após a realização bem sucedida do processo de mudança DEVE ser gerada uma copia de segurança do ambiente.

A copia de segurança gerada antes do processo de mudança NÃO DEVE ser apagada, devendo esta ser guardada no mínimo por um tempo variável entre uma semana e um mês para fins de Roll Back.

5 Procedimento de gerenciamento de patches

5.1 Objetivo

Definir procedimentos mais rápidos e simples para aplicação de atualizações de software de forma a não utilizar o procedimento padrão de gestão de mudanças.

5.2 Escopo e Aplicação

Estes procedimentos se aplicam unicamente a sistemas e softwares de mercado.

5.2.1 Estações de trabalho

Para estações de trabalho o procedimento de atualização DEVE ser aplicado logo após a disponibilização do fabricante, se possível por meio de atualização automática.

5.2.2 Servidores e outros equipamentos de rede

Para servidores e outros equipamentos de rede DEVEM no mínimo ser aplicados os seguintes procedimentos:

5.3 Procedimento operacional

5.3.1 Planejamento

As correções DEVEM ser planejadas, aprovadas, testadas de forma apropriada à complexidade e à sensibilidade dos sistemas afetados.

5.3.2 Validação da necessidade de atualização

Antes de dar inicio a qualquer atividade de implementação DEVE ser avaliada a documentação disponibilizada pelo fabricante, considerando o contexto do sistema e das aplicações, verificando os seguintes elementos:

- Verificar se a atualização tem utilidade ou se de alguma forma interessa o sistema em questão;
- Análise de Impacto da atualização e avaliação de eventuais efeitos colaterais;

5.3.3 Homologação da atualização

Para serviços críticos é recomendável que haja um processo de homologação para atualizações que acarretarem em modificações significativas.

As atualizações DEVEM assim ser testadas e avaliadas em sistemas de teste antes de serem instalados em produção para validar eventuais impactos negativos.

5.3.4 Medidas compensatórias

Quando for avaliada a possibilidade que uma atualização possa produzir um impacto negativo, é necessário considerar o uso de controles compensatórios tais como:

- A desativação do serviço afetado ou a alteração de parâmetros funcionais relacionados à falha tratada pela atualização;
- A adaptação ou agregação de controles adicionais finalizados a reduzir o impacto da ação da falha;
- Aumento do monitoramento para detectar ou prevenir a exploração da falha;
- Aumento da conscientização sobre a falha.

5.3.5 Efetivação da mudança

O responsável de T.I. DEVE dar inicio ao processo na data e horário que possuir o menor efeito possível nos serviços e DEVE acompanhar o processo de atualização ate o final.

5.3.6 Revisão Pós-Implementação

Ao final da atualização DEVEM ser aplicados os procedimentos definidos para validar a funcionalidade dos sistemas atualizados e dos sistemas relacionados.

Caso não seja possível resolver os problemas detectados na janela de tempo definida DEVE ser disparado o procedimento de Roll Back.

5.3.7 Procedimento de Roll Back

O procedimento de Roll Back deve restaurar o ambiente na configuração anterior a aplicação da mudança.

Desta forma a aplicação da atualização DEVE ser desfeita de forma a restaurar o estado anterior.

Em caso de necessidade de Roll Back, a ultima versão da cópia de segurança poderá ser utilizada para a restauração do sistema.

5.3.8 Cópias de segurança

Antes de realizar qualquer operação de atualização DEVE ser realizada uma copia de segurança do ambiente.

6 Procedimento de sincronismo de relógio

6.1 Objetivo

Definir o procedimento de sincronismo de relógio do sistemas de TI para SREI.

6.2 Aplicabilidade

Aplicabilidade: Todos os sistemas de TI do SREI, incluindo entre ele servidores, estações, equipamentos de rede e de proteção de perímetro.

6.3 Definições

- Servidor Master de Relógio: sistema conectado a Internet que atualiza periodicamente o próprio relógio com fontes confiáveis na Internet. Este sistema é a referencia primaria de hora para toda a rede do SREI e fornece o horário para todos os sistema.
- NTP: Protocolo para sincronismo de hora via rede TCP/IP utilizado para garantir o sincronismo do horário com relação a fontes confiáveis de hora.

6.4 Procedimentos

6.4.1 Servidor Máster

- Para redes com grande numero de sistemas recomenda-se definir um servidor especifico, localizado na DMZ, como servidor máster de relógio;
- Este servidor será assim a fonte de referencia para a hora de todos os outros sistemas da rede, devendo estes estar apontados para receber a hora do servidor máster;
- O servidor Master por sua vez DEVE buscar por meio da Internet a hora em servidores confiáveis, como da observatório nacional;

6.4.2 Sincronização de relógios:

- Todos os sistemas DEVEM ser configurados para sincronizar a hora usando do protocolo NTP;
- Todos os sistemas DEVEM receber informações de tempo de uma única fonte temporal, podendo ser local com servidor máster ou na Internet;
- Os procedimentos de Instalação e Configuração dos sistemas DEVEM contemplar as configurações necessárias para habilitação do serviço de tempo.
- O padrão de tempo acordado e utilizado corresponde ao UTC - Coordinated Universal Time;
- Configurações adequadas devem garantir que estão sendo levadas em consideração as especificações locais, dentre elas as que refletem as questões relacionadas ao horário de verão.
- No firewall de Internet DEVEM ser configuradas regras de acessos especificas para os servidores externos de tempo, a fim de evitar ações maliciosas de alteração de relógio.

7 Controle contra códigos maliciosos

DEVEM ser implementados controles técnicos e procedimentais adequados (incluindo software "antivírus", direitos de acesso limitados, conscientização em segurança e controles de gerenciamento de mudanças) para minimizar os riscos relacionados a ação de softwares maliciosos e outros softwares indesejados como vírus, worms, trojans, bombas lógicas, spams, adware e spyware.

Desta forma DEVEM ser no mínimo aplicados os seguintes recursos:

7.1 Software Antivirus

- DEVE ser instalado um software antivírus de mercado em todas as plataformas de TI aplicáveis, contemplando no mínimo todos os servidores e as estações de trabalho e os eventuais equipamentos moveis.
- Este software DEVE ser configurado para garantir uma proteção otimizada e DEVE ser atualizado assim que novas assinaturas são liberadas.
- O software de antivírus escolhido DEVE garantir que atualização das assinaturas tinha no Maximo periodicidade diária.
- Somente os responsáveis da área de TI podem instalar e configurar o software, DEVENDO ser impedido a outros colaboradores alterar ou interferir com a configuração, o processo de atualização e a operação do software antivírus.
- Mensagens e anexos de e-mail devem ser verificados rotineira e automaticamente por softwares maliciosos antes de seu uso. Controles de antivírus devem ser implementados em múltiplas camadas como gateways de e-mail, servidores e estações de trabalho e computadores portáteis.

7.2 Procedimentos complementares

- DEVE ser permitida somente a instalação de software regularmente licenciado;
- Softwares não autorizados e não licenciados NÃO DEVEM ser instalados nos sistemas.
- DEVE haver um processo para homologação e aprovação de softwares que inclua todas as formas de software como softwares comerciais, sistemas operacionais, utilitários, shareware e freeware e softwares para testes.
- A área de TI é responsável por conscientizar os usuários dos sistemas quanto aos riscos relacionados ao uso de software não aprovados e a ação de programas maliciosos e de vírus.