MINISTÉRIO PÚBLICO DA UNIÃO
MINISTÉRIO PÚBLICO MILITAR
PROCURADORIA-GERAL DE JUSTIÇA MILITAR

Portaria nº 12 /PGJM, de 01 de fevereiro de 2017.

Dispõe sobre os Procedimentos do Processo Ágil de Desenvolvimento de Software (PDS) e do Plano de Continuidade de Negócios (PCN), no âmbito do Ministério Público Militar.

O **PROCURADOR-GERAL DE JUSTIÇA MILITAR**, no uso das atribuições que lhe são conferidas pelo art. 124, inciso XX, da Lei Complementar nº 75, de 20 de maio de 1993,

CONSIDERANDO o disposto na Política de Tecnologia da Informação e Comunicação, ***resolve***:

Art.1º. Aprovar o Processo Ágil de Desenvolvimento de Software do Ministério Público Militar (PDS-MPM Ágil), na forma do ANEXO I da presente Portaria.

Art. 2º. Aprovar o Plano de Continuidade de Negócios do Ministério Público Militar (PCN-MPM), na forma do ANEXO II da presente Portaria.

Art. 3º. Esta Portaria entrará em vigor na data de sua publicação.

ANEXO I

Processo Ágil de Desenvolvimento de Software do Ministério Público Militar (PDS-MPM Ágil)

1 – Introdução

Este documento visa apresentar um resumo da Metodologia de Desenvolvimento Ágil, apoiada por Scrum – um *framework* (caixa de ferramentas) de desenvolvimento iterativo e incremental, hoje em utilização na Divisão de Desenvolvimento de Sistemas - DDS.

Todo o desenvolvimento é feito por meio de iterações e o esforço é orientado de forma que seja apresentado um novo conjunto de funcionalidades ao final de cada uma. Cada iteração tem um período de tempo definido, o que pode variar de projeto a projeto (a duração sugerida é de 15 dias por iteração).

Como prega o Scrum, seu foco está em definir práticas e posturas a serem adotadas durante o desenvolvimento, e não em definir processos especificamente.

2 – Definições

Ambiente corporativo: o ambiente corporativo para publicação de aplicações é composto pelos ambientes de fábrica, integração, homologação e produção. Cada um desses ambientes possui uma finalidade e é utilizado em um determinado momento do projeto. Por exemplo, o ambiente de homologação é usado para a execução de testes junto ao usuário do produto.

Ciclo de liberação: dentro do ciclo completo de desenvolvimento ágil de software, temos ciclos menores cujo escopo é parte do produto. Cada uma destas divisões é o ciclo de liberação, cujo objetivo é entrega de um incremento do produto, ou a liberação de uma versão do produto. O Ciclo de liberação inicia-se com a reunião de planejamento, onde o product backlog é estimado pela equipe e priorizado pelo product owner. É subdividido em iterações, em que as histórias da liberação serão subdivididas em tarefas para implementação. Encerra-se com a apresentação dos produtos gerados. Podem ocorrer diversos ciclos de liberação, com duração fixa.

Condução de reuniões: técnica utilizada pelo moderador da reunião a fim de mantê-la participativa, rica em ideias, sem fugir ao tema, visando o alcance de seu objetivo.

Débito técnico: pendências técnicas introduzidas no código em virtude de o mesmo ter sido implementado sem o design ou cuidados necessários. Estas pendências podem estar relacionadas com qualidade, bom design que permita fácil adaptação e manutenção, testes, etc. A existência de débito técnico indica que a tarefa não foi totalmente concluída e que a equipe deverá ter mais trabalho futuramente em virtude destas pendências deixadas no projeto.

Defeito: problema no software que faz com que ele se comporte de forma distinta da esperada/desejada.

Documento de Visão: documento que contém as informações identificadas durante o entendimento da demanda para viabilizar o início do desenvolvimento de software.

Equipe auto gerenciável: esta denominação enfatiza a característica da equipe de projeto de atuar na regulação de uma grande série de fatores que afetam a organização do trabalho.

Esforço: qualquer unidade, da preferência da equipe, usada para medir a quantidade de esforço envolvido na história. Exemplos: story points, horas, dias ideais, etc.

História de usuário (user story): descrição curta de uma característica do produto contada na perspectiva do usuário, utilizando uma linguagem comum ao negócio.

Histórias candidatas à iteração: histórias com maior prioridade que não foram implementadas ou que não foram concluídas na iteração anterior.

Impedimento: qualquer obstáculo ou problema que impeça um membro da equipe de concluir uma tarefa.

Incremento de produto de software: acréscimo de funcionalidades do produto de software final que é gerada a cada liberação. O incremento de produto de software deve ser algo observável e, preferencialmente funcional, para que o product owner e demais usuários possam experimentá-lo da forma mais realista possível.

Iteração: um ciclo de desenvolvimento, de duração fixa e curta, que corresponde a uma subdivisão da liberação e que produz uma versão estável e executável do produto de software.

Liberação: é a entrega de uma versão do produto de software, publicada no ambiente corporativo e que deve conter um conjunto mínimo de funcionalidades úteis para o negócio.

Objetivo da iteração: breve descrição do que a equipe pretende alcançar durante a iteração.

Objetivo da liberação: breve descrição do que a equipe pretende alcançar durante a liberação.

Prática: é uma técnica bem-sucedida de desenvolvimento de software que as equipes aplicam no seu dia a dia para executarem suas tarefas. É clara e objetiva e oferece um ponto de partida para obterem-se benefícios já experimentados largamente, mostrando-se bom exemplo a ser seguido no desenvolvimento ágil.

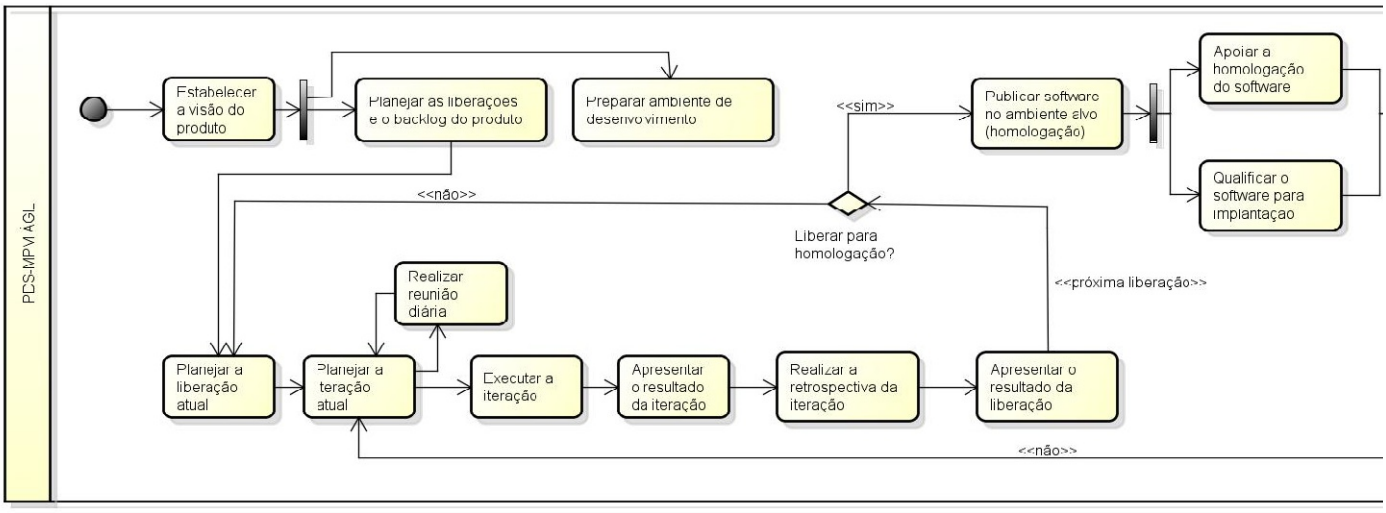
Pronto: uma liberação ou história está pronta (concluída) quando atende a todos os critérios de aceitação definidos pela equipe do projeto.

Stakeholder: indivíduo ou organização que tem um direito, ação, declaração ou interesse no software em desenvolvimento; envolvido; interessado.

Velocidade: medida da quantidade de trabalho que uma equipe consegue executar em um período de tempo determinado. É variável e específica para cada equipe de projeto. Só pode ser identificada após algumas semanas de trabalho, quando a equipe se torna mais integrada e inteirada do negócio do sistema e do processo de desenvolvimento.

Visão do produto: descrição concisa que comunica as principais características do produto de software. É o norte do projeto e orienta a identificação de suas funcionalidades.

3 – Fluxo do PDS-MPM Ágil



4 – Processo

4.1 Objetivo

O objetivo do Processo Ágil de Desenvolvimento de Sistemas do Ministério Público Militar (PDS-MPM Ágil) é guiar o desenvolvimento e a manutenção de sistemas corporativos no MPM visando a construção do produto de software que atenda à demanda do órgão e com qualidade. Complementando a Metodologia de Desenvolvimento de Sistemas – MDS Ver. 2.0 de 2012 que descreve os principais artefatos a serem confeccionados na produção de um projeto de software, respeitando as diferenças e adequações de cada projeto e equipe.

4.2 Escopo

O PDS-MPM Ágil tem como escopo o desenvolvimento de sistemas corporativos do MPM e as manutenções que contém mudanças significativas, de qualquer natureza. No caso de subcontratação o processo se aplica às atividades realizadas internamente para casos de integração.

4.3 Resultados esperados

Como resultados do uso bem-sucedido do processo:

a) O produto de software é desenvolvido alinhado às necessidades do negócio;

b) O produto de software entrega o maior valor possível para o negócio com qualidade;

c) O processo de trabalho da equipe do projeto é adaptado continuamente;

d) As entregas de software são frequentes;

e) Os riscos são identificados e tratados;

f) A equipe do projeto trabalha colaborativamente;

g) Os envolvidos têm visibilidade do progresso do projeto;

h) A documentação do software é automatizada e mantém-se sempre atualizada;

i) A documentação para transferência do conhecimento é gerada.

4.4 Papéis

Product owner (PO): indivíduo que representa os interesses dos stakeholders de negócio; deve ter conhecimento suficiente do negócio para responder aos questionamentos da equipe de desenvolvimento.

As características recomendadas para que o product owner desempenhe com sucesso o seu papel são:

a) Conhecer o processo de negócio e seus objetivos;

b) Gerenciar as expectativas dos stakeholders;

c) Comunicar e negociar;

d) Trabalhar em equipe;

e) Aceitar mudanças;

f) Ter iniciativa.

Scrum Master: indivíduo experiente no processo ágil que zela pela sua correta execução e ajuda os desenvolvedores a implementar software de alta qualidade alinhado às necessidades dos stakeholders; é um mentor que trabalha lado a lado com os outros membros da equipe de desenvolvimento em suas tarefas, disseminando as práticas do processo. É o líder técnico da equipe. Também resolve os impedimentos da equipe de desenvolvimento, executa as funções administrativas e acompanha o andamento do projeto.

As características recomendadas para que o Scrum Master desempenhe com sucesso o seu papel são:

a) Conhecer o processo ágil de desenvolvimento de software;

b) Comunicar e negociar;

c) Gerenciar conflitos e expectativas;

d) Liderar;

e) Trabalhar em equipe;

f) Ter iniciativa.

Desenvolvedor: indivíduo que constrói o produto de software.

As características recomendadas para que o desenvolvedor desempenhe com sucesso o seu papel são:

a) Conhecer o processo e as práticas de desenvolvimento ágil;

b) Conhecer os padrões do MPM;

c) Comunicar e negociar;

d) Trabalhar em equipe;

e) Aceitar mudanças;

f) Ter iniciativa.

Equipe de desenvolvimento: equipe formada por membros da Divisão de Desenvolvimento de Sistemas - DDS, responsável pela construção do produto de software. É composta pelo Scrum Master e desenvolvedores.

As características recomendadas para que a equipe de desenvolvimento desempenhe com sucesso o seu papel são:

a) Ser auto gerenciável;

b) Ser multidisciplinar;

c) Ter os requisitos específicos de cada papel que compõe a equipe.

4.5 Produtos de trabalho

Quadro Scrum (Jira): quadro representativo do estado das histórias, tarefas, ou outros elementos do processo com a finalidade de comunicar aos participantes o andamento do progresso do projeto.

Backlog da iteração: lista de histórias e de tarefas a serem executadas na iteração. É um subconjunto do backlog da liberação.

Backlog da liberação: lista de histórias previstas para uma liberação. É um subconjunto do backlog do produto.

Backlog do produto (product backlog): lista priorizada das características desejadas para o produto de software, representadas por meio de histórias de usuário.

Equipe do projeto: equipe formada pelo product owner e pela equipe de desenvolvimento. As características recomendadas para que a equipe do projeto desempenhe com sucesso o seu papel é atender às características de cada papel.

Demanda de TI: requisição de TI registrada no Jira.

Documento de Arquitetura: contém o registro das decisões arquiteturais do projeto.

Documento de Visão: contém as informações identificadas durante o entendimento das necessidades de negócio e as características do produto de software que atenderá

a estas necessidades.

Manual de usuário: orientação ao usuário sobre a forma de utilização do software, que pode se apresentar na forma de livro, ajuda do sistema, instalador etc.

Produto de software: conjunto de programas de computador (código fonte, testes automatizados, scripts de banco de dados, testes e operação), procedimentos, documentação e dados associados.

5 Atividades

5.1. Estabelecer a visão do produto

Descrição

Ocorre no início da execução do projeto, em uma reunião de aproximadamente duas horas com a participação da equipe do projeto e convidados, se necessário.

Entradas

Documento de Visão (com as informações sobre os envolvidos e a visão de negócio).

Saídas

Documento de Visão (com a declaração da visão do produto).

5.2. Planejar as liberações e o backlog do produto

Descrição

O product owner deve identificar, em conjunto com a equipe de desenvolvimento, as histórias do backlog do produto que compõem cada liberação;

Entradas

Backlog.

Saídas

Plano de liberações;

Backlog do produto.

5.3 Preparar ambiente de desenvolvimento

Descrição

Esta atividade é pré-requisito para o início da implementação do software.

Entradas

Tarefas

O scrum master deve realizar a criação do repositório no serviço de versionamento atualmente em uso, bem como a criação do projeto no sistema de acompanhamento e gerenciamento das demandas.

Saídas

Repositório e projeto criados.

5.4 Planejar a liberação atual

Descrição

O planejamento da liberação é feito em uma reunião de aproximadamente duas horas, no início de cada ciclo de liberação, e conta com a participação de toda a equipe do projeto.

Entradas

Backlog do produto.

Tarefas

O product owner deve revisar o objetivo da liberação atual.

Saídas

Backlog da Liberação.

5.5 Planejar a iteração atual

Descrição

O planejamento da iteração é feito em uma reunião de aproximadamente uma hora, no início de cada iteração, conta com a participação de toda a equipe do projeto.

Entradas

Backlog da Liberação;

Lista de ocorrências, defeitos e débitos técnicos (chamados no Jira).

Tarefas

O product owner deve informar à equipe de desenvolvimento as histórias candidatas, ou seja, confirmar aquelas que estão no topo do backlog.

Saídas

Backlog da Iteração;

Ambiente informativo atualizado (quadro no Jira).

5.6 Executar a iteração

Descrição

É o dia a dia da equipe do projeto durante todo o ciclo do desenvolvimento do software. A duração da iteração é definida pela equipe do projeto. As equipes têm trabalhado com a duração de duas semanas. Nesta atividade o produto de software é efetivamente produzido.

Entradas

Backlog da iteração;

Produto de software.

Tarefas

a) A equipe de desenvolvimento deve gerir o backlog da iteração;

b) A equipe de desenvolvimento deve selecionar as próximas tarefas do backlog da iteração a serem executadas.

Saídas

Produto de software;

Ambiente informativo atualizado (quadro Jira).

5.7 Realizar reunião diária

Descrição

A reunião deve ser realizada diariamente, em horário fixo definido pela equipe, com duração de até 15 minutos. A equipe de desenvolvimento participa em pé e deve ter acesso ao ambiente informativo do projeto. Caso as equipes tenham menos de 3 membros, pode-se realizar apenas a reunião de início e de fim da iteração. Uma vez que o processo de comunicação fica facilitado pelo acompanhamento no Jira.

Saídas

Ambiente informativo atualizado.

5.8 Apresentar o resultado da iteração

Descrição

Reunião, geralmente de até uma hora, realizada ao final de cada iteração, na qual a equipe de desenvolvimento apresenta o resultado do trabalho da iteração ao Product Owner, e eventuais stakeholders e usuários por ele convidados.

Entradas

Backlog da iteração;

Produto de software.

Saídas

Backlog do produto atualizado.

5.9 Realizar a retrospectiva da iteração

Descrição

Reunião, de até meia hora geralmente, realizada imediatamente após a reunião de apresentação de cada iteração, na qual a equipe de projeto avalia a execução da iteração.

Entradas

Tarefas

a) A equipe do projeto deve identificar os pontos positivos e negativos observados durante a execução da iteração;

b) A equipe do projeto deve identificar a causa raiz dos pontos negativos levantados;

c) A equipe do projeto deve propor soluções para as causas raiz identificadas.

Saídas

Melhorias no processo;

Jira atualizado.

5.10 Apresentar o resultado da liberação

Descrição

Reunião, de até duas horas geralmente, realizada ao final de cada liberação, na qual o product owner apresenta o resultado da liberação aos stakeholders e usuários por ele convidados.

Entradas

Backlog da liberação;

Produto de software.

Tarefas

a) O product owner deve apresentar o objetivo da liberação.

Saídas

Backlog do produto atualizado;

Plano de liberações atualizado.

5.11 Publicar o software no ambiente alvo

Descrição

É a disponibilização para uso do produto de software feita pela equipe de desenvolvimento usando o Publicador de Aplicações Jenkins.

Ao final de cada liberação, o software é disponibilizado para o ambiente de homologação e após a homologação do software, para o ambiente de produção.

Entradas

Plano de liberações;

Produto de software.

Tarefas

a) A equipe de desenvolvimento deve disparar o evento na ferramenta de integração para publicação da versão atual.

Saídas

Produto de software publicado.

5.12 Qualificar o software para implantação

Descrição

Verificação de conformidade com requisitos não funcionais feita obrigatoriamente antes da primeira publicação no ambiente de produção e sempre que mudanças significativas ocorrerem.

Entradas

Produto de software

Tarefa

a) A equipe de desenvolvimento deve registrar as ocorrências e defeitos verificados.

Saídas

Produto de software qualificado;

Lista de ocorrências e defeitos.

5.13 Apoiar a homologação do software

Descrição

Criação das condições necessárias à realização da homologação pelos usuários do produto de software, antes e durante a homologação de uma liberação. Envolve toda a equipe do projeto e tem duração variável.

Entradas

Produto de software.

Tarefas

a) A equipe de desenvolvimento deve verificar o ambiente de homologação disponibilizado ao usuário;

b) O product owner deve selecionar um grupo representativo de usuários para realizar a homologação do software;

c) O product owner deve apoiar a homologação do software pelos usuários;

d) A equipe de desenvolvimento deve garantir a estabilidade do ambiente e do software durante o período de homologação.

Saídas

Produto de software homologado;

Lista de ocorrências e defeitos.

ANEXO II

Plano de Continuidade de Negócios do Ministério Público Militar (PCN-MPM)

1. Definição de Plano de Continuidade de Negócios (PCN)

Plano de Continuidade de Negócios (PCN) é o processo de gestão da capacidade de uma organização de conseguir manter um nível de funcionamento adequado até o retorno à situação normal, após a ocorrência de incidentes e interrupções de negócios críticos.

O PCN deve ser desenvolvido preventivamente a partir de um conjunto de estratégias e planos táticos capazes de permitir o planejamento e a garantia dos serviços essenciais, devidamente identificados e preservados. Este processo orienta e define como e quais ações devem ser executadas para que se construa uma resiliência organizacional capaz de responder efetivamente e salvaguardar os negócios.

2. Objetivo

O PCN tem como objetivo especificar as ameaças e riscos identificados na organização e analisar os impactos no negócio, caso essas ameaças se concretizem. Visa com isso tornar possível seu funcionamento em um nível aceitável nas situações de contingência, resguardando os interesses dos intervenientes, a reputação, a imagem da organização e suas atividades-fim de significativo valor agregado.

3. Benefícios da Adoção de um PCN

A adoção de um Plano de Continuidade de Negócios é importante para a boa gestão e traduz-se em benefícios, tais como:

- Identificação de processos críticos e do impacto de ruptura em toda a entidade;
- Conhecimento do grau de exposição ao risco;
- Resposta eficiente às interrupções, sobretudo em função de um planejamento das ações necessárias;
- Treinamento do pessoal envolvido na resposta a ocorrências de impactos relevantes;
- Preservação da reputação da entidade no que tange a uma administração profissional na gestão, em caso de ruptura;
- Minimização de possíveis impactos às partes interessadas e ao patrimônio;
- Significativo aumento da probabilidade de sobrevivência da entidade ou do negócio em caso de uma crise, quaisquer que sejam as suas causas.

4. Diretrizes

A administração e os demais colaboradores da organização devem conhecer as fases do desenvolvimento do PCN e contribuir para a identificação das ameaças e dos riscos que podem afetar o negócio, mas que não constam do Plano.

O PCN deve ser elaborado inicialmente considerando as situações de risco com maior impacto e ampliar-se conforme a maturidade da organização frente à proteção dos seus ativos.

O treinamento e a conscientização de todos os colaboradores são de grande importância, permitindo que a organização gerencie os riscos, esteja preparada para os momentos de contingência e garanta a continuidade do negócio.

Dentro deste contexto, todos os colaboradores de uma entidade devem observar as práticas de segurança que possam contribuir no processo de gestão eficaz de continuidade de negócios.

5. Análise e Gestão de Riscos, Parecer Técnico e Risco de Perda de Dados

Organizações de todos os tipos e tamanhos enfrentam influências efatores internos e externos que tornam incerto se e quando elas atingirão seus objetivos. O efeito que essa incerteza tem sobre os objetivos da organização é chamado de risco.

Todas as atividades de uma organização envolvem risco. As organizações gerenciam o risco, identificando-o, analisando-o e, em seguida, avaliando se o risco deve ser modificado pelo tratamento do risco a fim de atender a seus critérios de risco. Ao longo de todo este processo, elas comunicam e consultam as partes interessadas, e monitoram e analisam criticamente o risco e os controles que o modificam, com o propósito de assegurar que nenhum tratamento de risco adicional seja requerido.

Embora todas as organizações gerenciem os riscos em algum grau, a norma ISO 31000/2009 recomenda que as organizações desenvolvam, implementem e aprimorem continuamente de forma a integrar o processo para gerenciar riscos na governança, estratégia e planejamento, gestão, processos de reportar dados e resultados, politicas, valores e cultura em toda a organização.

5.1 Termos e definições

Risco: Efeito da incerteza nos objetivos.

Efeito: Efeito é um desvio em relação ao esperado, pode ser positivo e/ou negativo.

Objetivos: Os objetivos podem ter diferentes aspectos (metas financeiras, de segurança, ambiental, etc), podem aplicar-se a diferentes níveis (estratégico, projeto e processo).

Os objetivos da Gestão de Riscos possibilitam:

- Identificar seus riscos;
- Priorizá-los em ordem de importância;
- Assegurar que estão gerenciados apropriadamente.

Princípios da Gestão de Riscos:

- Criar valor;
- Ser parte integrante processos organizacionais;
- Fazer parte da tomada de decisões;
- Abordar explicitamente a incerteza;
- Ser sistemática, estruturada e oportuna;
- Basear-se nas melhores informações disponíveis;
- Ser feita sob medida;
- Considerar fatores humanos e culturais;
- Ser transparente e inclusiva;
- Ser dinâmica, iterativa e capaz de reagir a mudanças;
- Facilitar a melhoria continua da organização.

Benefícios da Gestão de Riscos:

- Aumentar a probabilidade de atingir os objetivos;
- Encorajar a gestão proativa;
- Identificar e tratar riscos em toda a organização;
- Melhorar a identificação de ameaças e oportunidades;
- Atender às normas, requisitos legais e regulamentares;
- Melhorar o reporte de informações financeiras;
- Melhorar a governança;
- Melhorar a confiança das partes interessadas;
- Estabelecer base confiável para a tomada de decisão e para o planejamento.

Escopo

Avaliar a possibilidade da perda de dados decorrente de negligência ou falhas, analisando os controles existentes para a continuidade de negócios, orientados pelas melhores práticas baseadas nas normas PAS 200:2011 e ISO 22301:2013

5.2 Fatores de Riscos

FR1. Pane elétrica na rede externa.

Controles:

De forma a garantir a redundância de fontes de energia para atender exclusivamente os equipamentos do CPD, existe um grupo gerador com: um conjunto de baterias nobreak para atender as estações e servidores; dois geradores; e mais um nobreak instalado. **Existe procedimento documentado para o desligamento e posterior ligamento de todos os equipamentos alocados no CPD.**

FR2. Pane na infraestrutura de rede e servidores.

Controles:

Servidores que hospedam serviços críticos estão hospedados em sistema de virtualização com alta disponibilidade e em *cluster*.

No caso de pane no *switch* central (*core*), a operação é feita de modo redundante, ou seja, na falha de um equipamento, outro assume a função. Para atendimento a equipamentos de ativos de rede com defeito, existe contrato de manutenção corretiva e preventiva.

FR3. Falha em backup de base de dados e arquivos.

Controles:

A rotina de backup inclui realização de backup das bases de dados críticas de hora em hora. Para maiores informações verificar política de backup.

FR4. Interceptação das comunicações.

Controles:

Existe segmentação da rede da PGJM em VLANs contemplando cada área da PGJM. O tráfego entre as VLANS PGJM, PJM, internet e servidores de rede é controlado por *Firewall NG* com detecção de intrusão.

A grande maioria dos sistemas são acessados por comunicação criptografada e os demais estão em fase de migração para o HTTPS. Todos os acessos a sistemas utilizam autenticação em controladores de domínio utilizando método de autenticação Kerberos.

FR5. Pane em servidor localizado nas PJM.

Controle:

Em caso de pane no circuito de comunicação da PJM, o servidor instalado fisicamente na localidade remota se encarregará de distribuir endereços IP, armazenar os arquivos e autenticar os usuários no domínio.

No caso de pane do servidor local, a contingência é realizada por meio dos serviços de distribuição de endereços, servidor de arquivos e autenticação de usuários localizados na PGJM. Para isto, a infraestrutura de comunicação de dados do MPM já está preparada para redirecionar as comunicações.

FR6. Pane na comunicação do Storage.

Controle:

Existe redundância cruzada nas comunicações entre o Storage e os servidores que armazenam dados na solução.

FR7. Pane no Storage.

Controle:

O sistema de baterias interno do storage garante o funcionamento do equipamento por um período de 5 minutos, para o registro das últimas transações em memória.

Existe também contrato de manutenção e sistema de monitoramento remoto ativo e preditivo a falhas ligado direto ao fabricante.

FR8. Falha na restauração de backup.

Controle:

Existe política de backup e as restaurações, na maioria das vezes, são solicitadas pelo usuário por meio de sistema de controle de chamados e formulário aprovado, conforme estabelecido na política de backup e recuperação de arquivos.

FR9. Falta de homologação, testes do sistema e solicitação de inclusão na produção de forma urgente por parte da área gestora. Negligência por parte da área gestora do sistema.

Controle:

Se faz necessário a obediência a um fluxo mínimo de testes e homologação. Existe servidor SVN e Jenkins para deploy de aplicações.

FR10. Negligência pela falta de capacidade operacional e técnica dos envolvidos.

Controle:

Existe sistema automatizado de monitoramento e abertura de chamados automáticos, tanto para o contrato dos ativos que suportam a rede MPLS, quanto para os serviços e servidores da rede da PGJM. Sistema em fase de desenvolvimento e ajustes contínuos (PDCA), visto que não existe equipe dedicada ao monitoramento, assim como não existe equipe dedicada ao banco de dados. Atualmente, o sistema de monitoramento é frequentemente utilizado para monitorar serviços essenciais como, DNS, DHCP, HTTP, HTTPS, SMTP, validade dos certificados, *switchs, core*, espaço em disco de servidor de banco de dados, roteadores e servidores das PJM e da PGJM. Para os sistemas Linux, são também utilizados *scripts de logwatch*, reportando atividades, atualizações e tentativas de acesso, assim como elevação de privilégios. Para o servidor de arquivos, está ativado o serviço de *File Screening* em determinadas pastas.

FR11. Má utilização dos recursos de rede e TI.

Controle:

Existe portaria regulamentando o acesso aos recursos de TI que obriga o preenchimento e assinatura do termo de responsabilidade para acesso e cadastro de novos usuários.

Existe portaria regulamentando o acesso a rede sem fio e à internet, controlados por meio de sistemas de Webfilter tanto nas PJM (via Claro/Embratel) como na PGJM (*Firewall NG e Webfilter*).

A proteção da estações de trabalho de todas as localidades é realizada por solução de *antimalware* gerenciada centralmente.

6. Matriz de Exposição ao Risco

Fonto do Risco	Probabilidade	Consequência	PxC	Controle	N.Probabilidade	N.Consequência	N.PxC
FR1.Pane elétrica da rede externa	3	8	24	S	3	2	6
FR2.Pane na infraestrutura de rede e servidores	2	2	4	S	2	2	4
FR3.Falha em backup de base de dados e arquivos.	3	2	6	S	2	2	4
FR4.Interceptação das comunicações	1	16	16	S	1	8	8
FR5.Pane em servidor localizado nas PJMs	3	2	6	S	2	1	2
Pane de comunicação do Storage — FR6.	2	8	16	S	2	2	4
Pane no Storage — FR7.	1	16	16	S	1	8	8
FR8.Restauração de backup	2	4	8	S	2	2	4
FR9.Aplicação desenvolvida sem testes e/ou homologação	5	16	80	S	5	8	40
FR10.Negligência pela falta de capacidade operacional e técnica dos envolvidos	1	8	8	S	1	2	2
FR11.Má utilização dos recursos de rede e TI	4	8	32	S	4	4	16

Tabela de Probabilidade

NÍVEL	DESCRITOR	PROBABILIDADE
5	Quase certo	Espera-se que ocorra na maioria das circunstancias.
4	Provável	Provavelmente ocorrerá na maioria das circunstancias.
3	Possível	Pode ocorrer em algum momento.
2	Impossível	Não se espera que ocorra.
1	Raro	Poderia ocorrer em circunstancias excepcionais.

Tabela Consequência

NÍVEL	DESCRITOR	CONSEQUÊNCIA
1	Desprezível	Não afeta o alcance dos objetivos
2	Menor	Impede o alcance dos objetivos por período curto.
4	Moderada	Impede o alcance de um objetivo por

		período longo.
8	Maior	Impede o alcance de vários objetivos por período longo.
16	Catastrófica	Perdas enormes, impacto em toda a organização

7. ANEXOS

7.1 Desligar CPD

7.1.1 Observações importantes:

- O serviço de DNS está rodando em uma máquina física, então não deve ser desligado primeiro, pois alguns serviços são dependentes desse serviço.
- Existe um servidor físico de AD no CPD e outro no *Datacenter* da Embratel, então "em tese" é possível desligar o servidor de AD físico do CPD.

7.1.2 Ordem básica do desligamento

Obs: Acesse a Wiki com a lista de servidores;

Obs2: Se você se deparar com algum servidor com update pendente, não instale, pois pode comprometer a velocidade do desligamento

1. Máquinas físicas (não virtuais);

2. Máquinas com virtualização - desligue as máquinas virtuais primeiro;

3. Quando se deparar com o servidor de monitoramento execute:

- *omd stop* (na linha de comando);
- Depois execute o *shutdown* normal.

4. Servidores 04 e 05 podem ser desligados na sequência já que possuem serviço de DNS;

5. Servidor Exchange:

- Srv (08,12) são as databases do Exchange. Observar a migração das caixas e depois desligar;
- Srv23 somente deve ser desligado após as databases

6. Nodes dos *cluster Hyper-V.*

- De pause no cluster e depois *stop*.

7. Após todas as máquinas estarem desligadas, passe para a parte de infraestrutura (*switchs,* roteador, *core e storage*).

8. Desligue o *switch* de fibra para garantir que nenhum serviço esteja acessando o *Storage*;

9. Desligar o *Storage*:

- Comece pelos botões externos (1,2);
- Desligue *o standby power supply* (3,4) –parte interna;
- Desligue as réguas (5,6,7,8,9,10) –parte interna.

10. Desligar *Core* - desligue no botão e remova os cabos;

11. Switchs do *rack* CPD;

12. Firewalls;

13. Telefonia:

- Desligar os disjuntores na parte traseira;
- Disjuntores vermelhos e azul.

14. Desligar o ROTEADOR Embratel.

7.2 Ligar CPD

7.2.1 Observações importantes.

- O serviço de *Active Directory* é altamente dependente de DNS, então após ligar a infraestrutura básica de rede (roteador, *switch* e *core*), o primeiro serviço a subir deve ser o DNS.
- Atualmente o SRV11 depende de compartilhamento que está no 01.

7.2.2 Ordem básica para inicializar

1. Roteador;

2. Core

Atenção!! Observar as luzes das *blades* do *core*. Caso fiquem vermelhas, saque *a blade* e coloque novamente, e observe.

3. Firewall;

4. DNS (15 e 51);

5. Switch;

6. Storage (mesma sequencia do desligamento);

a) Disjuntores externos;

b) Réguas internas;

c) Controller;

Observação: esperar que a numeração que aparece fique na cor azul e aparecendo na seguinte ordem:

De cima para baixo:

2 2 1 1 1 1 0 0	

Switch fibra

7. Ligar as réguas dos *racks*;

8. Jenkins (18);

9. 20;

10. Servidor de arquivos (01):

Característica: 4 discos de 1T e 2 de 146GB.

11. Biblioteca de backup (deve fazer todo o processo de scanner das fitas)

12. Vá ligando o resto srv12, 08, 22 etc;

13. Telefonia:

a) Ligar os disjuntores que estão na parte de trás, os vermelhos e azul.

14. HIPATH:

a) Navegar no KVM apertando os botões da *MasterView* e verificar se os servidores estão “subindo”;

15. Hiper-V (53)

a) Tirar do “pause” o cluster opções “Bring... e Resume.

16. Testar acessos e serviços;

7.3 Registro documental referente ao FR1 – Pane elétrica da rede externa