ANEXO Nº TRF2-ANE-2014/00079

Anexo ao documento

Data de revisão:	Revisão nº
Data de criação: 25/09/2014	DAL-TRF2-PlanoContinuidadeNegócios-1.00-2014

Plano de Continuidade de Negócios

1. Apresentação

Este documento acessório à Política de Segurança da Informação da Justiça Federal trata do PCN - Plano de Continuidade de Negócios.

2. Escopo

Esta Política, bem como os eventuais respectivos documentos anexos, têm abrangência local, ou seja, se aplicam exclusivamente no âmbito do Tribunal Regional Federal da 2ª Região.

3. Público-alvo

Esta Política, bem como os eventuais respectivos documentos anexos, se aplicam a todas as pessoas naturais e jurídicas na qualidade de agentes públicos em sentido amplo (ou seja, em sentido estrito ou equiparados), que exercem ou exerceram atividades na Justiça Federal da 2ª Região ou para ela, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, seja em cargo, emprego, função, mandato ou com mero múnus ou atribuição pública ou de interesse público, encontrando-se na atividade ou inatividade, o que inclui, dentre outros similares:

- servidores;

- empregados;

- magistrados;

- estagiários e aprendizes;

- partes em quaisquer contratos, convênios, acordos, ajustes, termos de parceria e outros instrumentos congêneres, bem como seus eventuais agentes (tais como empregados, prepostos, estagiários e aprendizes de "terceirizados");

- pensionistas de servidores e magistrados.

Esta Política, bem como os eventuais respectivos documentos anexos, também se aplicam a todos aqueles que, mesmo exercendo ou tendo exercido atividades na Justiça Federal da 2ª Região ou para ela sem qualquer forma de investidura ou vínculo, também possam eventualmente lidar com negócios, o que inclui, dentre outros similares:

- advogados (inclusive estagiários) e outras espécies de mandatários, bem como seus clientes;

- membros de outras instituições públicas (tais como OAB, AGU, DPU, MPF, CJF, CNJ, TCU, CEF e BB);

- visitantes.

4. Conceituação

Para os efeitos desta Política, considera-se continuidade de negócios a minimização, até um patamar

TRF2ANE201400079B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1281960-4419 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal 83 Tribunal Regional Federal - 2ª Região

emergencial aceitável de eficácia previamente definido, de qualquer suspensão ou interrupção, como reação ao incidente de segurança da informação que tenha lhe causado relevante impacto negativo, mediante a administração de crises, a manutenção de continuidade operacional e a recuperação de desastres.

5. Objetivos

Os objetivos desta Política são, essencialmente, assegurar os simultâneos acesso e proteção da informação com seus principais requisitos de segurança (ou seja, confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade), levando em consideração as vulnerabilidades exploráveis por ameaças e agressões com risco de impacto negativo, e tendo ênfase seletiva nos aspectos das seguranças física, lógica e de recursos humanos, descritas no item 8.1 do Anexo I da Resolução nº 6, de 7 de abril de 2008, do CJF.

Esta Política é complementada pelos demais documentos acessórios à Política de Segurança da Informação da Justiça Federal, com ênfase em outros aspectos.

6. Documentos de referência

Os documentos de referência desta Política são, principalmente, os seguintes:

- art. 13 da Resolução nº 90, de 29 de setembro de 2009, do CNJ;

- Anexo da Resolução nº 103, de 23 de abril de 2010, do CJF;

- art. 1º, § ún., da Resolução nº 176, de 10 de junho de 2013, do CNJ;

- Anexo da Resolução nº 91, de 29 de setembro de 2009, do CNJ;

- Anexos da Resolução Conjunta nº 4, de 28 de setembro de 2005, do CJF;

- "Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário" elaboradas pelo Comitê Nacional de Gestão de Tecnologia da Informação e Comunicação do Poder Judiciário;

- "Boas Práticas em Segurança da Informação" elaboradas pelo TCU;

- publicações do DSIC - Departamento de Segurança da Informação e Comunicações do GSI - Gabinete de Segurança Institucional da Presidência da República;

- Resolução nº 22, de 30 de maio de 2011, do Tribunal;

- Anexo da Portaria nº 124, de 10 de abril de 2013, do CJF.

Além desses, os documentos de referência desta Política são, especialmente, os seguintes:

- art. 2º, c/c os itens 4.2 e 9.3.4 do Anexo I, da Resolução nº 6, de 7 de abril de 2008, do CJF;

- arts. 42 e ss. da Resolução nº 4, de 14 de março de 2008, do CJF;

- Resolução nº 188, de 10 de fevereiro de 2012, do CJF;

- arts. 37, *caput*, IX, e 93, XII, da CRFB;

- Lei nº 7.783, de 28 de junho de 1989;

- arts. 73 e 74 da Lei nº 8.112, de 11 de dezembro de 1990;

- Lei nº 8.745, de 9 de dezembro de 1993;

- Lei nº 12.608, de 10 de abril de 2012;

- Decreto nº 7.257, de 4 de agosto de 2010;

TRF2ANE201400079B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1281960-4419 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal 84 Tribunal Regional Federal - 2ª Região

- Decreto nº 7.777, de 24 de julho de 2012;

- legislação especial;

- Resolução nº 71, de 31 de março de 2009, do CNJ;

- arts. 9º e ss. da Resolução nº 185, de 18 de dezembro de 2013, do CNJ;

- Recomendação nº 40, de 13 de junho de 2012, do CNJ;

- art. 14 da Resolução nº 35, de 19 de outubro de 2009, do Tribunal;

- Resolução nº 1, de 3 de fevereiro de 2010, do Tribunal;

- Resolução nº 10, de 8 de julho de 2010, do Tribunal;

- art. 5º da Resolução nº 32, de 11 de junho de 2012, do Tribunal;

- Resolução nº 119, de 27 de dezembro de 2012, do Tribunal;

- Resolução nº 13, de 30 de junho de 2014, do Tribunal;

- publicações do CERT.br, da RNP - Rede Nacional de Ensino e Pesquisa e do CTIR - Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal do DSIC-GSI da Presidência da República.

7. Disposições gerais

7.1. Dos incidentes de segurança da informação que justificam a execução do PCN

7.1.1. O PCN deverá ser executado diante de todo incidente de segurança da informação que tenha causado relevante impacto negativo ao negócio, assim considerado aquele que ocasionar a suspensão ou interrupção deste por um período superior ao TOR - tempo objetivo de recuperação, o que inclui, dentre outros similares:

- prática não permitida ou proibida, em um contexto de inobservância da Política de Segurança da Informação da Justiça Federal;

- força maior (tal como incêndio; panes elétrica, mecânica, hidráulica, telefônica, telemática ou estrutural; enchente, inundação ou alagamento; vandalismo etc.);

- paralização ou greve na prestação dos serviços da Justiça Federal da 2ª Região;

- paralização ou greve envolvendo a prestação de serviço de interesse da Justiça Federal da 2ª Região (tal como bancos, correios, transportes públicos, manutenção de elevadores, manutenção de *hardware* ou *software*, segurança privada, fornecimento de água para consumo humano, fornecimento de insumos primordiais para os serviços da Justiça Federal da 2ª Região etc.);

- suspensão ou interrupção, por outro motivo, da prestação dos serviços da Justiça Federal da 2ª Região, ou de serviço público essencial ou de outra espécie de serviço de interesse da Justiça Federal da 2ª Região.

7.1.2. O TOR referido no item 7.1.1 desta Política é o tempo razoável pré-definido no qual o negócio deverá estar novamente em um patamar emergencial aceitável de eficácia previamente definido, após sua suspensão ou interrupção.

7.1.3. Para o fim de definição, para cada negócio, do TOR descrito no item 7.1.2 desta Política, aplicam-se subsidiariamente os tempos de urgência definidos para a classificação de informações conforme os respectivos subníveis, e os tempos definidos em outras regras especiais de continuidade de negócios (tais como os concernentes a plantão judiciário, indisponibilidade de sistemas eletrônicos, dispensa de licitação etc.).

7.1.4. Todos os negócios deverão se submeter a mapeamento e conseqüentes definições do respectivo TOR descrito no item 7.1.2 desta Política, pelos respectivos GNs, em conjunto com as unidades técnicas pertinentes.

TRF2ANE201400079B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1281960-4419 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal 85 Tribunal Regional Federal - 2ª Região

7.1.5. Durante a preparação, execução e exaurimento do PCN, poderá ser mantido estreito intercâmbio com o CRI-Jus e outras CLRIs, bem como com o CERT.br, a RNP - Rede Nacional de Ensino e Pesquisa e o CTIR - Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal do DSIC-GSI da Presidência da República.

7.2. Da preparação do PCN

7.2.1. Todos os meios de contato de cada um dos membros da CLRI (ou seja, número de telefone fixo, número de fax, número de telefone celular, nomes em mensageiros instantâneos, *e-mails* etc.) deverão ser compartilhados entre si.

7.2.2. A CLRI deverá ter um único ponto de contato de cada espécie, de fácil memorização, o qual deverá constar, clara e ostensivamente, em posições relevantes de qualquer local, físico ou eletrônico, do Tribunal.

7.2.3. Os pontos de contato das unidades responsáveis pela TI, e pela infraestrutura, telefonia ou segurança, servirão, subsidiariamente, à CLRI.

7.2.4. Deverão constar, clara e ostensivamente, em posições relevantes de qualquer local, físico ou eletrônico, do Tribunal, para a CLRI e as unidades técnicas pertinentes, os pontos de contato:

- das próprias unidades técnicas pertinentes;

- do SAMU - Serviço de Atendimento Móvel de Urgência;

- do CBMERJ - Corpo de Bombeiros Militar do Estado do RJ;

- da SEDEC - Secretaria de Estado de Defesa Civil do Estado do RJ;

- da PM/RJ - Polícia Militar do Estado do RJ;

- da PC/RJ - Polícia Civil do Estado do RJ;

- do DPF;

- da GM-Rio - Guarda Municipal do Rio de Janeiro;

- da CET-Rio - Companhia de Engenharia de Tráfego do Rio de Janeiro;

- de cada prestador de serviço público essencial ou de outra espécie de serviço de interesse da Justiça Federal da 2ª Região.

7.2.5. Qualquer incidente que tenha causado relevante impacto negativo deverá ser imediatamente reportado, por quem tomar conhecimento, ou de modo automatizado, ao respectivo GN e, daí, à CLRI, para os devidos fins.

7.2.6. Toda notificação deverá ser cadastrada no registro de incidentes de segurança da informação, e todo incidente deverá ser classificado de acordo com as métricas definidas pelo CSI-Jus, para os devidos fins, inclusive histórico e estatístico.

7.2.7. Caso as métricas referidas no item 7.2.6 desta Política ainda não tenham sido definidas, poderão ser utilizadas as métricas equivalentes em vigor.

7.2.8. Os registros de incidentes das unidades responsáveis pela TI, e pela infraestrutura, telefonia ou segurança, servirão, subsidiariamente, à CLRI.

7.2.9. Aplicam-se subsidiariamente o processo de gestão de riscos e o Catálogo de Fraudes do CAIS - Centro de Atendimento a Incidentes de Segurança da RNP.

7.3. Da execução do PCN

7.3.1. O PCN em sentido amplo é estruturado, nessa ordem, pelo:

- PGI - Plano de Gerenciamento de Incidentes (ou PAC - Plano de Administração de Crises), cujo escopo é a organização da gestão e tranqüilização do público interno e externo;

TRF2ANE201400079B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1281960-4419 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal 86 Tribunal Regional Federal - 2ª Região

- PCN - Plano de Continuidade de Negócios em sentido estrito (ou PCO - Plano de Continuidade Operacional), cujo escopo é a eficácia do negócio e aumento da resiliência; e

- PRN - Plano de Recuperação de Negócios (ou PRD - Plano de Recuperação de Desastres), cujo escopo é a normalidade do negócio e consolidação da resiliência.

7.3.2. O início da execução do PGI deverá se dar, pela CLRI, sob coordenação da CLSI, em conjunto com os respectivos GNs e as unidades técnicas pertinentes, e com a ciência da Presidência do Tribunal, a partir do fim do TOR descrito no item 7.1.2 desta Política.

7.3.3. Os respectivos GNs deverão evitar, sempre que possível, o início da execução do PGI.

7.3.4. Se o incidente tiver atingido parâmetros de relevância definidos pelo CSI-Jus, a CLRI solicitará auxílio ao CRI-Jus, bem como a qualquer outra instituição pertinente, para os devidos fins.

7.3.5. Caso os parâmetros referidos no item 7.3.4 desta Política ainda não tenham sido definidos, poderão ser utilizados os parâmetros equivalentes em vigor.

7.3.6. O PGI consiste, nessa ordem, em:

- análise da causa do incidente (ou seja, a agressão), concernente a sua materialidade e autoria;

- análise dos efeitos do incidente (ou seja, o impacto), na forma de uma AIN - avaliação de impacto no negócio (*BIA - business impact assessment*), concernente aos negócios descontinuados, bem como ao tipo e extensão do impacto;

- análise do registro de incidentes de segurança da informação;

- projeção e escolha de meios de cessação da causa e dos efeitos do incidente;

- implementação dos meios escolhidos;

- difusão de esclarecimentos e alertas, clara e ostensivamente, pela unidade responsável pela comunicação social, caso não se trate de informação classificada em qualquer grau de sigilo, conforme a Lei nº 12.527, de 18 de novembro de 2011;

- triagem e ordenação dos negócios descontinuados, conforme os respectivos níveis de prioridade;

- coordenação das respostas ao incidente a serem providenciadas pelas unidades técnicas pertinentes;

- início da elaboração do PCN em sentido estrito.

7.3.7. Para o fim de definição, para cada negócio, do nível de prioridade referido no item 7.3.6 desta Política, aplicam-se subsidiariamente os níveis de prioridade definidos para a classificação de informações conforme os respectivos subníveis, e os níveis de prioridade definidos em outras regras especiais de continuidade de negócios (tais como os concernentes a greve, situação de emergência, estado de calamidade pública etc.).

7.3.8. Todos os negócios deverão se submeter a mapeamento e conseqüentes definições do respectivo nível de prioridade referido no item 7.3.6 desta Política, pelos respectivos GNs, em conjunto com as unidades técnicas pertinentes.

7.3.9. O PCN em sentido estrito consiste, nessa ordem, em:

- triagem e ordenação da recuperação (ou seja, a reação), conforme a ordem de prioridade dos negócios descontinuados referida no item 7.3.6 desta Política;

- projeção e escolha de soluções alternativas adaptativas, equivalentes, em termos de eficácia, a cada negócio sob normalidade (ou seja, "plano B", "plano C" etc.), conforme suas respectivas peculiaridades, considerando-se os custos e benefícios;

- definição, para cada negócio, do patamar emergencial aceitável de eficácia;

- implementação das soluções escolhidas, mesmo sem a conclusão das etapas descritas no item 7.3.6

TRF2ANE201400079B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1281960-4419 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal 87 Tribunal Regional Federal - 2ª Região

desta Política;

- difusão de mais esclarecimentos e alertas, clara e ostensivamente, pela unidade responsável pela comunicação social, com a mesma ressalva constante no item 7.3.6 desta Política;

- motivação por meio da identidade institucional;

- relatório e cadastramento dos resultados do PCN em sentido estrito.

- início da elaboração do PRN.

7.3.10. As soluções referidas no item 7.3.9 poderão consistir, dentre outras correlatas, no seguinte:

- um certificado digital no lugar de outro;

- assinatura física no lugar da eletrônica;

- teletrabalho, videoconferência ou sessão de julgamento "virtual" no lugar das respectivas formas presenciais;

- plantão judiciário ou serviço extraordinário no lugar do expediente forense normal;

- contratação por tempo determinado para atender a necessidade temporária de excepcional interesse público;

- um ramal telefônico no lugar de outro;

- fax no lugar do *e-mail* ou SIGA, ou vice-versa;

- malote físico no lugar do Malote Digital;

- peticionamento físico no lugar do eletrônico;

- documento físico no lugar do eletrônico;

- procedimento manual no lugar do automatizado;

- um local de guarda no lugar de outro;

- transferência temporária de sede;

- *hot site*, *warm site* e *cold site*;

- sistema de som ambiente no lugar do aviso rolante no portal do Tribunal na Intranet;

- realocação de recursos, inclusive mediante contratação ou acordo de reciprocidade;

- "caminhão-pipa";

- gerador;

- dispensa no lugar de licitação.

7.3.11. O PRN consiste, nessa ordem, em:

- análise do relatório referido no item 7.3.9 desta Política;

- seguimento da ordenação descrita no item 7.3.9 desta Política;

- projeção e escolha de soluções para a retomada do patamar original ou aproximado de normalidade de cada negócio, contando-se com meios de armazenamento, preferencialmente *offsite*, dotados de alta disponibilidade e redundância capazes de viabilizar a recuperação de cópias de segurança (*backups*);

TRF2ANE201400079B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1281960-4419 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal 88 Tribunal Regional Federal - 2ª Região

- implementação das soluções escolhidas, preferencialmente em consonância com o processo de gestão de riscos;

- difusão de mais esclarecimentos, clara e ostensivamente, pela unidade responsável pela comunicação social, com a mesma ressalva constante no item 7.3.6 desta Política;

- mais motivação por meio da identidade institucional;

- relatório e cadastramento dos resultados do PRN.

7.4. Do exaurimento do PCN

7.4.1. Além do intercâmbio descrito no item 7.1.5 desta Política, deverá ser encaminhada cópia do relatório referido no item 7.3.11 da mesma à CLSI, para análise, bem como à Presidência do Tribunal, para ciência.

7.4.2. Deverá ser preparado e executado plano de teste periódico do PCN, conforme o grau de complexidade e realidade, nessa ordem, na forma de:

- simples revisão (*checklist*);

- descrição verbal das atividades em grupo (*walkthrough* ou "teste de mesa");

- simulação; ou

- suspensão real.

7.4.3. Além das regras concernentes ao próprio PCN, a preparação do plano de teste periódico também envolve:

- a definição da parte do PCN objeto do teste;

- a definição dos parâmetros mínimos do teste;

- a forma de observação e avaliação do objeto do teste;

- a divulgação da realização do teste às unidades pertinentes, com a mesma ressalva constante no item 7.3.6 desta Política.

7.4.4. Aplicam-se subsidiariamente os mecanismos de controle típicos da Política de Segurança da Informação da Justiça Federal, o processo de gestão de riscos e os testes usualmente realizados pelas unidades técnicas pertinentes (tal como simulação de combate a incêndio, simulação de escape, *pentest* etc.).

8. Disposições finais

8.1. As unidades responsáveis deverão providenciar os pertinentes registros e divulgação das informações de que trata esta Política, incluindo a ciência ao CSI-Jus e a consolidação das mesmas na página da segurança da informação, constante no portal eletrônico do Tribunal, sem prejuízo dos pertinentes meios oficiais de publicação.

.

SERGIO SCHWAITZER
PRESIDENTE

TRF2ANE201400079B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1281960-4419 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action