PODER JUDICIÁRIO
JUSTIÇA FEDERAL

TRIBUNAL REGIONAL FEDERAL DA 2ª REGIÃO

PORTARIA PRES/TRF2 Nº 340, DE 29 DE MAIO DE 2025

Institui o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ) no âmbito da Justiça Federal da 2ª Região.

O PRESIDENTE DO TRIBUNAL REGIONAL FEDERAL DA 2ª REGIÃO, no uso de suas atribuições,

CONSIDERANDO a Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO o Anexo I da Portaria CNJ nº 162, de 10 de junho de 2021, que estabelece o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ);

CONSIDERANDO a Norma ABNT NBR ISO/IEC 27035:2021, que define requisitos para gestão de incidentes de segurança da informação;

CONSIDERANDO o aumento dos incidentes cibernéticos na rede mundial de computadores e a necessidade de processos voltados à gestão adequada da segurança da informação;

CONSIDERANDO a importância de uma atuação proativa frente a incidentes de segurança da informação;

RESOLVE, *ad referendum* do Órgão Especial:

CAPITULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Instituir o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário no âmbito da Justiça Federal da Segunda Região (JF2R), com os seguintes objetivos:

I – estabelecer diretrizes e procedimentos para a gestão de incidentes cibernéticos na JF2R, visando restaurar a operação normal dos serviços com a maior brevidade possível, minimizando os prejuízos à atividade da JF2R e atendendo os níveis de serviço acordados;

II – internalizar, no que for aplicável, no âmbito da JF2R, o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ), conforme Anexo I da Portaria CNJ nº 162, de 10 de junho de 2021.

Art. 2º O Protocolo de Prevenção de Incidentes Cibernéticos (PPINC-JF2R) é aplicável a todos os ativos de informação, projetos, processos e serviços de Tecnologia da Informação, abrangendo os servidores, colaboradores, órgãos e unidades da Justiça Federal da 2ª Região.

Parágrafo único. Os Protocolos de Investigação de Ilícitos Cibernéticos e os Protocolos para Gerenciamento de Crises Cibernéticas são complementares e se harmonizam com o Protocolo de Prevenção de Incidentes Cibernéticos.

Art. 3º São responsáveis pelo PPINC-JF2R:

I - Comissão Local de Resposta a Incidentes (CLRI), responsável pelo tratamento dos incidentes;

II – Assessoria de Gestão de Segurança da Informação (AGSI), responsável por analisar e responder a notificações e atividades relacionadas a incidentes de segurança cibernética;

III – Secretaria de Tecnologia da Informação (STI), incumbida de operacionalizar a detecção, o monitoramento e a recuperação dos incidentes.

Art. 4º Compete à Comissão Local de Resposta a Incidentes (CLRI):

I – assegurar a identificação, registro e avaliação dos incidentes em tempo hábil, com adoção de medidas de contenção e/ou solução adequada;

II – solicitar apoio multidisciplinar abrangendo as áreas de tecnologia da informação, segurança da informação, jurídica, pesquisas judiciárias, comunicação, controle interno, segurança institucional, entre outras, necessárias para responder aos incidentes de segurança de maneira adequada e tempestiva.

Parágrafo único. A CLRI terá autonomia compartilhada no tratamento de incidentes cibernéticos, não podendo intervir diretamente nos ativos impactados, devendo obter as autorizações necessárias através de seu presidente.

Art. 5º Constituem diretrizes do PPINC-JF2R:

I – implementar medidas preventivas para evitar incidentes cibernéticos, em conformidade com as normas ISO/IEC 27035;

II – integrar as funções de identificar, proteger, detectar, responder e recuperar incidentes, conforme estabelecido pelo PPINC-PJ;

III – assegurar que os incidentes abrangidos sejam eventos, confirmados ou suspeitos, que comprometam os ativos de informação, dados e processos de trabalho relativos ao ambiente tecnológico da JF2R;

IV – analisar os incidentes que resultem em degradação, interrupção ou indisponibilidade de serviço essencial, vulnerabilidades, divulgação, alteração ou destruição de informações, bem como a prática de ato definido como crime ou infração administrativa.

Art. 6º Para a implementação do PPINC-JF2R, deverão ser observados os seguintes princípios críticos:

I – base de conhecimento de defesa: utilização de informações obtidas por meio de interações com outras equipes de tratamento de incidentes e respostas;

II – instrumentos de medição e métricas: definição e estabelecimento de métricas comuns para avaliar a eficácia da segurança no Tribunal (Anexo III);

III – prevenção: monitoramento contínuo dos ativos tecnológicos, realização de campanhas para disseminação da cultura de segurança cibernética, implementação de controles proativos e priorização na revisão de processos para mitigação de riscos;

IV – formação e capacitação: processos formais de educação continuada, integrados em planos de capacitação, que incluam a disseminação, formação e instrução de todos os envolvidos, direta ou indiretamente, em atividades que promovam a cultura de segurança cibernética na organização. Tais instrumentos deverão ser revisados periodicamente;

V – resiliência: capacidade de recuperação rápida e minimização de impactos operacionais;

VI – conformidade: alinhamento às normas e regulamentações nacionais, incluindo a Lei Geral de Proteção de Dados (LGPD).

CAPÍTULO II

DAS ETAPAS DO TRATAMENTO DE INCIDENTES

Art. 7º As etapas do tratamento de incidentes cibernéticos são:

I – detecção e registro;

II – classificação;

III – investigação e contenção;

IV – recuperação;

V– encerramento;
VI – avaliação.

Seção I

Detecção e registro

Art. 8º Detecção e Registro referem-se ao recebimento do incidente, sua anotação e as autorizações necessárias para o encaminhamento da investigação.

§ 1º Todos os incidentes, sejam notificados ou detectados, devem ser registrados para garantir a manutenção do histórico e auxiliar na geração de indicadores, por meio da elaboração do Relatório de Incidentes de Segurança da Informação (RISI).

§ 2º A comunicação deve incluir a identificação do usuário e uma descrição detalhada do ocorrido, exceto nos casos em que a notificação seja realizada de forma anônima por meio da Central de Serviços de TI.

§ 3º A comunicação do incidente, interna ou externa, deve ser registrada por qualquer usuário o mais brevemente possível, conforme as seguintes diretrizes:

I) internamente, por meio da Central de Serviços de TI, através do telefone (21) 2282-8022, pela abertura de chamado na intranet no endereço http://chamados.trf2.jus.br ou pelo SEI, iniciando um novo processo do tipo RISI;

I) externamente, através dos e-mails agsi@trf2.jus.br, abuse@trf2.jus.br e tiajuda@trf2.jus.br.

§ 4º As vulnerabilidades ou fragilidades suspeitas não devem ser objeto de teste ou prova pelos usuários, sob pena de violação das normas e regulamentações de segurança da informação que regem a Instituição ou de causar danos aos recursos de TI.

Seção I

Classificação

Art. 9º A etapa de Classificação consiste na avaliação do impacto e priorização de incidentes com base em sua criticidade, conforme especificado nos Anexos I e II deste Protocolo.

Seção III

Investigação e Contenção

Art. 10. A etapa de Investigação compreende a investigação, o tratamento do incidente, a coleta de dados, a comunicação às áreas afetadas e a proposição e aplicação de ações de contenção, quando necessário.

§ 1º A investigação e o tratamento de incidentes devem ser realizados de forma a garantir a disponibilidade, integridade, confidencialidade e autenticidade da informação, visando ao retorno das operações à normalidade no menor prazo possível e minimização de futuras ocorrências, por meio da proposição de medidas corretivas, quando cabíveis.

§ 2º A CLRI/TRF2 é responsável pela investigação de incidentes e artefatos maliciosos, bem como pela proposição e implementação das ações de contenção.

§ 3º A coleta de evidências relacionadas aos incidentes de segurança da informação deve ser realizada por pessoal designado pela CLRI/TRF2.

§4º Nos casos em que o incidente cibernético estiver vinculado a suspeitas de descumprimento das normas e regulamentações de segurança da informação, o sigilo deverá ser mantido durante todo o processo de investigação, restringindo o acesso às evidências, informações e registros apenas aos envolvidos.

§5º A investigação deverá ser formalmente autorizada pelo Comitê Local de Segurança da Informação (CLSI).

§6º Na ocorrência de indícios de ilícitos durante a gestão de incidentes de segurança da informação, a Presidência do TRF2 e a CLSI deverão ser notificadas para a avaliação das medidas

cabíveis.

Seção IV

Recuperação

Art. 11. etapa de Recuperação visa restabelecer os serviços afetados e à comunicação com as partes interessadas.

Seção V

Encerramento

Art. 12. O Encerramento do incidente cibernético será realizado pela CLRI, que deverá notificar as demais partes interessadas.

Seção VI

Avaliação

Art. 13. Avaliação é o registro e análise do incidente, com o objetivo de identificar falhas, aprendizados e oportunidades de melhoria, ocorrendo ao final de todo o processo.

§ 1º O tratamento de incidentes cibernéticos deverá ser avaliado por meio do seu respectivo histórico, pela Assessoria de Gestão de Segurança da Informação (AGSI), com o apoio da CLRI, visando identificar oportunidades de aprimoramento.

§ 2º A CLSI e o Comitê de Segurança da Informação da Justiça Federal (CSI-Jus) deverão ser notificados sobre os incidentes ocorridos para fins de registro, estatística e apoio.

CAPÍTULO III

DISPOSIÇÕES FINAIS

Art. 14. O PPINC-JF2R deverá ser revisado e atualizado, no mínimo, a cada dois anos, ou quando necessário.

Art. 15. Os responsáveis pelo PPINC-JF2R deverão interagir com o Comitê de Resposta a Incidentes de Segurança da Informação da Justiça Federal - CRI-Jus, com as CLRIs de outros Tribunais e com o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR-Gov).

Art. 16. O descumprimento do PPINC-JF2R poderá acarretar sanções administrativas, civis ou criminais, conforme a gravidade do caso e as legislações aplicáveis.

Art. 17. Os casos omissos serão resolvidos pela Presidência deste Tribunal.

Art. 18. Esta Portaria entra em vigor na data de sua publicação.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.

LUIZ PAULO DA SILVA ARAÚJO FILHO
Presidente

Documento assinado eletronicamente por **LUIZ PAULO DA SILVA ARAÚJO FILHO**, **Presidente**, em 30/05/2025, às 15:17, conforme art. 1º, III, "b", da Lei 11.419/2006.

ANEXO I

Classificação de Incidentes de Segurança da Informação

1. Objetivo

Apresentar a classificação detalhada dos tipos de incidentes de segurança da informação e cibernética que podem ocorrer na JF2R, com o objetivo de facilitar sua identificação, priorização e tratamento.

2. Categorias de Incidentes de Segurança da Informação

2.1. Conteúdo Abusivo

Incidentes relacionados à disseminação de materiais inadequados ou ilegais, que podem comprometer a reputação ou integridade da JF2R.

· **Spam:**

Descrição: Mensagens indesejadas, enviadas em massa, geralmente para fins comerciais ou maliciosos.

Exemplo: Recebimento de e-mails com links de phishing ou propagandas de serviços não solicitados.

Impacto: Congestionamento de caixas de entrada, redução de produtividade e risco de exposição a ataques.

· **Assédio Virtual:**

Descrição: Ataques direcionados a indivíduos, como difamação, discriminação ou perseguição.

Exemplo: E-mails ou mensagens em sistemas internos contendo insultos ou ameaças.

Impacto: Clima organizacional negativo, danos psicológicos e riscos legais.

· **Pornografia, Pedofilia ou Conteúdo Violento:**

Descrição: Compartilhamento de material explícito ou que incite violência.

Exemplo: Utilização indevida de e-mails corporativos para envio de vídeos de conteúdo inapropriado.

Impacto: Comprometimento ético, jurídico e reputacional.

· **Hoax (Boatos):**

Descrição: Mensagens alarmantes e falsas compartilhadas para enganar ou causar pânico.

Exemplo: Disseminação de e-mails indicando uma "ameaça cibernética crítica" inexistente.

Impacto: Perda de tempo e recursos na investigação de ameaças inexistentes.

2.2. Código Malicioso - Malware

Programas ou scripts criados para causar danos ou comprometer a segurança dos sistemas.

· **Vírus:**

Descrição: Código malicioso que infecta arquivos e se propaga ao ser executado.

Exemplo: Infecção de estações de trabalho por arquivos enviados por e-mail.

Impacto: Danos a arquivos, instabilidade no sistema e perda de dados.

· **Worms:**

Descrição: Programas autorreplicantes que consomem recursos de rede e sistemas.

Exemplo: Sobrecarga em servidores de e-mails devido a ataques massivos de worms.

Impacto: Redução de desempenho da rede e interrupção de serviços.

· **Trojan (Cavalo de Troia):**

Descrição: Software disfarçado como legítimo para acessar sistemas indevidamente.

Exemplo: Programas baixados de fontes desconhecidas contendo funcionalidades ocultas para roubo de dados.

Impacto: Comprometimento de credenciais e informações confidenciais.

· **Ransomware:**

Descrição: Software que sequestra dados e exige pagamento para liberá-los.

Exemplo: Bloqueio de arquivos críticos do Tribunal, com pedido de resgate em criptomoedas.

Impacto: Interrupção de atividades e potencial perda financeira.

· **Spyware:**

Descrição: Programas que coletam informações sem o consentimento do usuário.

Exemplo: Instalação de software espião em dispositivos corporativos.

Impacto: Violação de privacidade e exposição de informações sensíveis.

2.3. Intrusão

Incidentes de acesso não autorizado a sistemas, redes ou informações.

· **Acesso Não Autorizado:**

Descrição: Tentativa de explorar sistemas ou redes para obter acesso indevido.

Exemplo: Invasão por meio de senhas comprometidas.

Impacto: Violação de dados sensíveis, com potencial de dano jurídico e reputacional.

· **Exploração de Vulnerabilidades:**

Descrição: Uso de falhas técnicas para comprometer serviços ou dispositivos.

Exemplo: Ataques baseados em vulnerabilidades de software desatualizado.

Impacto: Danos a sistemas e interrupção de operações críticas.

2.4. Segurança da Informação

Comprometimento de dados ou informações críticas.

· **Exposição de Dados:**

Descrição: Divulgação acidental ou intencional de informações confidenciais.

Exemplo: Envio de documentos sigilosos por e-mail para destinatários incorretos.

Impacto: Comprometimento da confidencialidade e risco de ações judiciais.

· **Modificação Não Autorizada:**

Descrição: Alteração de dados sem permissão.

Exemplo: Manipulação indevida de registros em bases de dados judiciais.

Impacto: Perda de integridade e confiabilidade nos dados.

2.5. Fraudes

Incidentes que envolvem tentativa de enganar ou obter vantagens ilegais.

· **Phishing:**

Descrição: Engenharia social para obter credenciais ou dados sensíveis.

Exemplo: E-mails falsos simulando comunicações internas.

Impacto: Comprometimento de contas e violação de dados sensíveis.

· **Uso Indevido de Software:**

Descrição: Instalação ou distribuição de software pirata.

Exemplo: Utilização de aplicativos não licenciados em estações de trabalho.

Impacto: Risco legal e vulnerabilidades de segurança.

2.6. Interrupção de Serviços

Eventos que afetam a disponibilidade dos serviços de TI.

· **Negação de Serviço (DoS/DDoS):**

Descrição: Sobrecarga de sistemas para torná-los indisponíveis.

Exemplo: Ataques volumétricos em sites do Tribunal.

Impacto: Indisponibilidade de sistemas críticos e prejuízo à continuidade das atividades.

· **Falhas em Infraestrutura Crítica:**

Descrição: Interrupção de redes, servidores ou sistemas essenciais.

Exemplo: Falha em data centers que suporta os sistemas judiciais.

Impacto: Paralisação das operações e danos à imagem institucional.

2.7. Outros

Categoria destinada a incidentes atípicos ou fora do escopo das categorias acima.

Exemplo: Incidentes envolvendo dispositivos de IoT ou tecnologias emergentes ainda não cobertas pelas classificações tradicionais.

Impacto: Necessidade de adaptação e revisão contínua do protocolo.

Anexo II

Tabela de Nível de Criticidade de Incidentes Cibernéticos

Nível de Criticidade	Descrição do Impacto	Exemplos de Cenários	Ação Necessária
Muito Alta	Comprometimento grave da operação do tribunal, paralisação completa de serviços essenciais, ou perda irreparável de dados.	- Ataque ransomware que criptografa todos os sistemas críticos do tribunal. - Vazamento de dados sigilosos de processos judiciais. - Intrusão que compromete a integridade de decisões judiciais.	- Acionamento imediato do plano de resposta a incidentes. - Comunicação às autoridades e à alta gestão. - Mobilização de equipes de crise e especialistas externos.
Alta	Impacto significativo em sistemas críticos, mas com possibilidade de mitigação parcial e recuperação no curto prazo.	- Indisponibilidade de sistemas de consulta processual por horas. - Tentativa de phishing que resulta no comprometimento de credenciais de usuários privilegiados. - Ataques DDoS contra o portal do tribunal.	- Investigação urgente e contenção do incidente. - Reforço de segurança. - Notificação interna de impacto.
Média	Impacto moderado em serviços não críticos, com interrupções temporárias e risco limitado aos dados.	- Acesso não autorizado a contas de usuários comuns. - Falha técnica em sistemas de backup sem afetar os sistemas ativos. - Tentativa de exploração de vulnerabilidades mitigada a tempo.	- Resolução com prioridade moderada. - Monitoramento adicional dos sistemas afetados. - Revisão de políticas de segurança.
Baixa	Impacto mínimo ou nenhum impacto direto nos serviços ou dados do tribunal.	- E-mails de phishing detectados e bloqueados. - Tentativa de escaneamento de portas sem sucesso. - Pequenos erros em sistemas internos sem exposição de dados.	- Documentação do incidente. - Aplicação de correções preventivas. - Treinamento ou alerta para usuários sobre o ocorrido.

Anexo III

Indicadores de Performance e Monitoramento

1. Objetivo

Definir os indicadores que permitirão medir a eficácia das ações de prevenção, detecção

e resposta a incidentes de segurança da informação no âmbito da JF2R.

2. Indicadores Estratégicos

2.1. Número de Incidentes Reportados:

· **Descrição:** Quantidade total de incidentes registrados no período de análise.

· **Finalidade:** Monitorar a ocorrência de problemas e avaliar a eficácia das medidas preventivas.

2.2. Tempo Médio de Resposta (TMR):

· **Descrição:** Tempo médio decorrido entre a detecção e o início do tratamento do incidente.

· **Meta:** Reduzir progressivamente o TMR para incidentes críticos.

2.3. Taxa de Recuperação de Serviços (TRS):

· **Descrição:** Proporção de serviços afetados que foram restaurados dentro do prazo previsto.

· **Finalidade:** Avaliar a resiliência operacional.

2.4. Incidentes Reincidentes:

· **Descrição:** Percentual de incidentes que voltaram a ocorrer após ações corretivas.

· **Finalidade:** Medir a eficácia das soluções implementadas.

3. Indicadores Operacionais

3.1. Taxa de Detecção Antecipada:

· **Descrição:** Percentual de incidentes identificados antes de impactarem os serviços críticos.

· **Meta:** Aumentar continuamente esta taxa.

3.2. Nível de Conformidade:

· **Descrição:** Porcentagem de controles de segurança implementados conforme as normas ISO/IEC 27001 e 27002.

· **Finalidade:** Garantir alinhamento às melhores práticas.

3.3. Participação em Treinamentos:

· **Descrição:** Percentual de servidores e magistrados que participaram de treinamentos de segurança cibernética.

· **Meta:** Atingir 100% de adesão anual.

3.4. Incidentes por Categoria:

· **Descrição:** Distribuição percentual de incidentes por tipo (conteúdo abusivo, malware, etc.).

· **Finalidade:** Identificar tendências e categorias mais críticas para priorizar ações.

3.5. Taxa de Notificação Espontânea:

· **Descrição:** Percentual de incidentes reportados por usuários antes de serem detectados pelo monitoramento automatizado.

· **Finalidade:** Incentivar a cultura de reporte proativo.

4. Ferramentas de Monitoramento

4.1. Painéis de controle com dados em tempo real sobre incidentes.

4.2. Relatórios trimestrais com análises de tendências e recomendações.

4.3. Feedback dos usuários sobre a resposta aos incidentes reportados.