Art. 17º As lições aprendidas devem ser utilizadas para a elaboração ou revisão dos procedimentos específicos de resposta (playbook) e para a melhoria do processo de preparação para crises cibernéticas.
Art. 18º Deve ser elaborado relatório contendo a descrição e detalhamento da crise, bem como o plano de ação tomado para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados.
Art. 19º As ações de resposta e recuperação da crise cibernética devem observar, ainda, o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCC-PJ), constante do Anexo II da Portaria n. 162, de 2021, do CNJ.
Art. 20º O protocolo estabelecido nesta portaria será revisto anualmente ou, quando necessário, em menor prazo.
Art. 21º Esta Portaria entra em vigor na data de sua publicação.
Boa Vista/RR, 25 de janeiro de 2023.
Desembargador Leonardo Pache de Faria Cupello
Presidente do TRE/RR
(documento assinado eletronicamente)

Documento assinado eletronicamente por LEONARDO PACHE DE FARIA CUPELLO, Presidente, em 25/01/2023, às 14:03, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-rr.jus.br/autenticidade informando o código verificador 0757369 e o código CRC EFFB3E7A.

PORTARIA Nº 48/2023

Institui o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ) no âmbito do Tribunal Regional Eleitoral de Roraima.

O Presidente do Tribunal Regional Eleitoral de Roraima, no uso de suas atribuições legais e regimentais;
CONSIDERANDO a Resolução nº 396/2021 do Conselho Nacional de Justiça (CNJ), que Instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
CONSIDERANDO o anexo I da Portaria nº 162, de 10 de junho de 2021, do Conselho Nacional de Justiça, que constitui o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ);
CONSIDERANDO os anexos IV, V e VI da Portaria nº 162/2021, do Conselho Nacional de Justiça, que contêm os manuais referentes à Proteção de Infraestruturas Críticas de TIC, Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital e, ainda, Gestão de Identidades;
CONSIDERANDO os termos da Resolução CNJ nº 370/2021, que Instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTICJUD);
CONSIDERANDO a Norma ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro da organização;
CONSIDERANDO a Norma ABNT NBR ISO/IEC 27002:2022, que trata de princípios e diretrizes gerais para a Gestão da Segurança da Informação;
CONSIDERANDO o número crescente de incidentes cibernéticos no ambiente da rede mundial de computadores e a necessidade de processos de trabalho orientados para a boa gestão da segurança da informação;
CONSIDERANDO as boas práticas de Governança de Tecnologia da Informação e Comunicação (TIC) que visam garantir a disponibilidade e integridade dos ativos tecnológicos deste Tribunal;

CONSIDERANDO a necessidade de agir de forma proativa a incidentes de segurança da informação;
CONSIDERANDO o regramento da Política Segurança da Informação deste Tribunal Regional Eleitoral de Roraima,
RESOLVE:
Art. 1º Instituir o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ) no âmbito do Tribunal Regional Eleitoral de Roraima nos termos deste ato.
CAPÍTULO I
DISPOSIÇÕES PRELIMINARES
Art. 2º O Protocolo de Prevenção de Incidentes Cibernéticos do TRE/RR tem como objetivo:
I - prevenir incidentes cibernéticos por meio das funções identificar, proteger, detectar,responder e recuperar;
II - disciplinar o funcionamento da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) no âmbito do Tribunal Regional Eleitoral de Roraima;
III - promover alinhamento às normas, regulamentações e às melhores práticas, relacionadas à Gestão de Incidentes de Segurança da Informação;
IV - promover ações que contribuam para a resiliência dos serviços de Tecnologia da Informação a ataques cibernéticos.
Art. 3º Para os efeitos deste normativo, são estabelecidas as seguintes definições:
I - Ativo: qualquer coisa que represente valor para uma instituição, tal como a informação;
II - CGTIC: Comitê de Gestão de Tecnologia da Informação e Comunicação. É um comitê que tem como principal objetivo elaborar planos táticos e operacionais, análise técnica de demandas, acompanhamento da execução de planos, projetos e ações que envolvam tecnologia da informação e comunicação;
III - CSI: refere-se ao Comitê de Segurança da Informação que é uma equipe multidisciplinar, subordinada à Presidência, com responsabilidade de deliberar, conduzir e fiscalizar as ações de segurança da informação no TRE/RR;
IV - Controle: providência que modifica o risco, incluindo qualquer processo, política, dispositivo, prática ou ação;
V - ETIR: Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética. Denominação tradicionalmente atribuída a grupos de resposta a incidentes de segurança da informação, embora os incidentes não mais se limitem a tecnologia;
VI - Incidente de Segurança da Informação: evento que viola ou representa ameaça iminente de violação de política de segurança, de política de uso aceitável ou de prática de segurança padrão;
VII - PPINC-PJ: refere-se ao Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário definido pelo CNJ, que contempla conjunto de diretrizes para a prevenção de incidentes cibernéticos em seu mais alto nível;
VIII - Resiliência: poder de recuperação ou capacidade de determinada organização resistir aos efeitos de um incidente;
IX - Segurança Cibernética: é um conjunto de práticas que protege informação armazenada nos computadores e aparelhos de computação e transmitida através das redes de comunicação, incluindo a Internet e telefones celulares;
X - Segurança da Informação: refere-se a medidas que visam a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, incluindo a preservação da disponibilidade, da confidencialidade e da integridade das informações e dos sistemas; enquanto a Segurança Cibernética se aplica a uma parte da segurança da informação com foco na proteção

digital, cuidando das ameaças as informações transportadas por meios cibernéticos, a Segurança da Informação tem um foco mais amplo, cuidando da redução de riscos no transporte de dados por qualquer meio, seja digital ou não;

XI - Sistema de Gestão de Segurança da Informação (SGSI): políticas, procedimentos,manuais e recursos associados e atividades coletivamente.

Art. 4º Para implementação desta norma, deverão ser observados pelas áreas envolvidas os princípios críticos definidos no PPINC-PJ, que são:

I - uso de base de conhecimento de defesa;

II - priorização da segurança da informação;

III - definição e estabelecimento de métricas;

IV - diagnóstico contínuo;

V - formação e capacitação;

VI - busca de soluções automatizadas de segurança cibernética;

VII - resiliência.

CAPÍTULO II

COMPETÊNCIA DE ATUAÇÃO

Art. 5º Cabe à Presidência:

I - analisar as deliberações do Comitê de Segurança da Informação (CSI) sobre Gestão de Incidentes de Segurança da Informação e decidir sobre possíveis providências;

II - formalizar a aceitação da execução das ações propostas para conter ou prevenir incidentes de segurança da informação;

III - comunicar ao órgão de polícia judiciária com atribuição para apurar os fatos, na ocorrência de incidentes penalmente relevantes;

IV - acionar o Comitê de Crises Cibernéticas, nos termos do Protocolo de Gerenciamento de Crises Cibernéticas, quando necessário.

Art. 6º Cabe à Comissão de Segurança da Informação:

I - deliberar sobre as principais diretrizes e temas relacionados à Gestão de Incidentes de Segurança da Informação;

II - monitorar e avaliar periodicamente a estrutura de Gestão de Incidentes de Segurança da Informação e o sistema de controles internos, assim como propor melhorias consideradas necessárias;

III - aprovar formalmente o processo de Gestão de Incidentes de Segurança da Informação e suas futuras revisões;

IV - deliberar sobre ações de contenção ou Prevenção de Incidentes de Segurança da Informação;

V - manifestar-se sobre matérias atinentes à segurança da informação que lhe sejam submetidas;

VI - assessorar, em matérias correlatas, a Presidência do TRE/RR.

Art. 7º Cabe ao Comitê de Gestão de Tecnologia da Informação e Comunicação (CGTIC):

I - monitorar e comunicar à ETIR os Incidentes de segurança da informação dos ativos sob sua responsabilidade;

II - assegurar a implementação das ações e dos controles definidos para prevenção de contenção de incidentes de segurança da informação dos ativos sob sua responsabilidade.

Art. 8º Cabe à Coordenadoria de Infraestrutura e Cibersegurança (CIC):

I - coordenar a instituição, capacitação, implementação e manutenção da infraestrutura necessária à Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR);

II - garantir que os incidentes de segurança na rede do TRE/RR sejam devidamente tratados;

III - adotar procedimentos de *feedback* para assegurar que os usuários que comuniquem incidentes de segurança da informação na rede interna de computadores sejam informados dos procedimentos adotados;
IV - disseminar cultura voltada para comunicação de incidentes de segurança da informação;
V - subsidiar o Comissão de Segurança da Informação com informações pertinentes à estrutura de gestão de incidentes de segurança da informação;
VI - desenvolver, testar e implementar um Processo de Gestão de Incidentes de Segurança da Informação e garantir sua efetividade.
Art. 9º A Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) tem a responsabilidade de receber, analisar, classificar, tratar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores.
Art. 10º O funcionamento da ETIR do TRE/RR - definição da missão, público-alvo, modelo de implementação, nível de autonomia, integrantes, canais de comunicação de incidentes e os serviços a serem prestados deve ser regulado em norma específica.
CAPÍTULO III
DAS FUNÇÕES DO PROTOCOLO DE PREVENÇÃO A INCIDENTES CIBERNÉTICOS
Art. 11º São funções básicas do Protocolo de Prevenção a Incidentes Cibernéticos, conforme definição do PPINC-PJ, identificar, detectar, responder o incidente, proteger e recuperar a informação.
Seção I
Da Função Identificar
Art. 12º A função "Identificar" consiste na análise dos riscos de ataques cibernéticos a que sistemas, pessoas, dados, recursos e ativos de TI em geral estão expostos, incluindo a elaboração e a execução de um plano de tratamento dos riscos.
Art. 13º A função identificar é executada dentro do escopo do Processo de Gestão de Riscos de Segurança da Informação, instituído no Tribunal.
Seção II
Da Função Proteger
Art. 14º Consiste no desenvolvimento e na implementação de salvaguardas que assegurem a proteção de dados, inclusive pessoais, ativos de informação, bem como a prestação de serviços.
§ 1º A função "Proteger" deve ser implementada pelo conjunto mínimo de ações elencadas a seguir:
I - implantação e aprimoramento contínuo de um Sistema de Gestão de Segurança da Informação (SGSI) no TRE/RR;
II - controle de acesso e de utilização de recursos de TI;
III - cópia de segurança e de restauração de sistemas, aplicativos, dados e de documentos;
IV - plano de continuidade de TI dos serviços essenciais;
V - gestão de capacidade e disponibilidade de TI dos serviços essenciais;
VI - processo de gerenciamento de mudanças para todos os ativos de TI;
VII - gestão de vulnerabilidades técnicas dos serviços essenciais;
VIII - utilização de ferramenta de segurança para estações de trabalho, contendo, no mínimo, as funções de antivírus, automação de políticas de segurança de endpoint, proteção contra criptografia (ransomware), controle de aplicativos e de dispositivos removíveis;
IX - controle de acesso a conteúdo na internet (filtragem web);
X - utilização de ferramenta de segurança de rede *next generation firewall)* visando
XI - uso de antivírus de rede, sistema de detecção e prevenção de ameaças e implementação de redes privadas virtuais (VPN);

XII - integridade da rede protegida por meio da segmentação e segregação de ambientes, de maneira a estabelecer barreiras de contenção de danos em caso de comprometimento (sub-redes distintas por serviços) e para garantia de recursos para serviços prioritários (serviços essenciais, em detrimento de ambientes de laboratório/desenvolvimento/homologação);
XIII - promover campanha e/ou treinamento sobre segurança da informação para magistrados e servidores;
XIV - atualização tecnológica constante;
XV - implementação gradual dos controles de segurança da informação presentes na Norma NBR 27002;
XVI - implementação gradual dos controles mínimos recomendados no Manual de Referência para Proteção de Infraestruturas Críticas de TIC, editado pelo Conselho Nacional de Justiça, considerando a escala de aplicabilidade de cada controle em relação ao porte e maturidade do TRE /RR em segurança da informação;
XVII - implementação gradual dos requisitos de resiliência cibernética recomendados no Manual de Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital, editado pelo Conselho Nacional de Justiça, considerando a aplicabilidade dos requisitos em relação ao porte e maturidade do TRE/RR em segurança da informação;
XVIII - implementação gradual dos requisitos de resiliência cibernética recomendados no Manual de Gestão de Identidade e de Controle de Acesso, editado pelo Conselho Nacional de Justiça, considerando a aplicabilidade dos requisitos em relação ao porte e maturidade do TRE/RR em segurança da informação;
XIX - implantação de uma Política de Educação e Cultura em Segurança Cibernética, conforme o anexo VII da Portaria nº 162, de 10 de junho de 2021 do Conselho Nacional de Justiça.
§ 2º As salvaguardas elencadas no § 1º deste artigo devem ser implementadas para todos os ativos de TIC, no que couber, considerados essenciais ou não ao negócio, permitindo variar quanto ao nível de implementação, de acordo com a natureza e criticidade do ativo.
§ 3º As atualizações dos ativos de TIC (pacotes de segurança, firmware, entre outros) devem ser aplicadas, sempre que possível, tão logo liberadas, mas considerando:
I - os riscos decorrentes da atualização;
II - os riscos decorrentes da não aplicação (ou postergação);
III - a criticidade do ativo;
IV - a estabilidade dos serviços.
Seção III
Das Funções Detectar, Responder e Recuperar
Art. 15º As atividades decorrentes das funções "Detectar", "Responder" e "Recuperar" do Protocolo de Prevenção de Incidentes Cibernéticos devem estar cobertas pelo Processo de Gestão de Incidentes de Segurança da Informação.
Art. 16º Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, deverá, ainda, ser seguido o Protocolo de Investigação para Ilícitos Cibernéticos.
Parágrafo único. Na ocorrência da hipótese prevista no caput deste artigo, o Comissão de Segurança da Informação e a Presidência do TRE/RR deverão ser comunicados.
Art. 17º Quando o incidente de segurança da informação decorrer de suspeita de descumprimento da Política de Segurança da Informação, será observado o sigilo durante todo o processo, ficando as evidências, informações e demais registros restritos aos envolvidos na investigação.
Art. 18º A gestão de incidentes de segurança cibernética deve ser realizada por meio do Processo de Gestão de Incidentes de Segurança da Informação, contendo as fases de detecção, triagem, análise e respostas aos incidentes de segurança.

Art. 19º As ações relacionadas à prevenção de incidentes devem observar, ainda, o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ), constante do Anexo I da Portaria nº 162, de 2021, do CNJ.
Art. 20º O protocolo estabelecido nesta portaria será revisto anualmente ou, quando necessário, em menor prazo.
Art. 21º Esta Portaria entra em vigor na data de sua publicação.
Boa Vista/RR, 25 de janeiro de 2023.
Desembargador Leonardo Pache de Faria Cupello
Presidente do TRE/RR
(documento assinado eletronicamente)

Documento assinado eletronicamente por LEONARDO PACHE DE FARIA CUPELLO, Presidente, em 25/01/2023, às 14:03, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-rr.jus.br/autenticidade informando o código verificador 0757364 e o código CRC 7CD12FB2.

TRAMITAÇÃO DE FEITOS

PAUTAS

PAUTA DE JULGAMENTO DA 9ª SESSÃO ORDINÁRIA DE 02.02.2023 - VIRTUAL NO PJE

A SECRETARIA JUDICIÁRIA DO TRIBUNAL REGIONAL ELEITORAL DE RORAIMA, EM OBEDIÊNCIA AO QUE DETERMINA O ARTIGO 18, PARÁGRAFO ÚNICO DA RESOLUÇÃO TSE N° 23.478/2015, COMBINADO COM O QUE DISPÕE A RESOLUÇÃO TRE-RR N° 421/2020, E DE ORDEM DO RELATOR, TORNA PÚBLICO QUE, NA SESSÃO ORDINÁRIA DO DIA 02.02.2023 SERÁ (ÃO) JULGADO (S) O (S) SEGUINTE (S) FEITO (S):
PRESTAÇÃO DE CONTAS ELEITORAIS (12193) - [Prestação de Contas - De Candidato, Cargo - Deputado Estadual]
Processo nº 0601063-94.2022.6.23.0000
Relator: Juiz Luiz Alberto de Morais Junior
Interessado: Eleição 2022 Clarice Custodio de Sousa Deputado Estadual, Clarice Custodio de Sousa
Advogados do(a) Interessado: Silvia Barros Ramalho Pimentel - RR1886, Cleber Silva Veras - RR2173, Frankembergen Galvao da Costa - RR1342
Link para Sustentação Oral: https://forms.gle/8hXAG8TzQJzkG4ds5
Modalidade de Julgamento: Virtual no PJe.
Horário: 10:00 às 23:59 Horas
PRESTAÇÃO DE CONTAS ELEITORAIS (12193) - [Prestação de Contas - De Candidato, Cargo - Deputado Federal]
Processo nº 0601126-22.2022.6.23.0000
Relator: Juiz Elvo Pigari Junior
Interessado: Eleição 2022 Cassia Rejane do Nascimento Deputado Federal, Cassia Rejane do Nascimento
Advogado do(a) Interessado: Massuhan Ferreira Alves - RR1846-A
Link para Sustentação Oral: https://forms.gle/8hXAG8TzQJzkG4ds5
Modalidade de Julgamento: Virtual no PJe.
Horário: 10:00 às 23:59 Horas