Caderno Administrativo
Tribunal Regional do Trabalho da 14ª Região

DIÁRIO ELETRÔNICO DA JUSTIÇA DO TRABALHO

PODER JUDICIÁRIO

REPÚBLICA FEDERATIVA DO BRASIL

Data da disponibilização: Segunda-feira, 03 de Junho de 2024.

Gabinete da Presidência

Portaria

Portaria de Regulamentação

PORTARIA GP N.º 0581, DE 29 DE MAIO DE 2024.

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO, no uso de suas atribuições legais e regimentais,
CONSIDERANDO a edição da Portaria GP n.º 0436, de 13/5/2021, e respectivos anexos, publicada no DEJT em 14/5/2021, que estabeleceu a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 14ª Região, da qual são parte integrante todas as normas e procedimentos complementares e afins editados pelo Tribunal e que tem como objetivo garantir um ambiente tecnológico controlado e seguro de forma a oferecer todas as informações necessárias aos processos deste Tribunal, com integridade, confidencialidade e disponibilidade;
CONSIDERANDO o teor da manifestação exarada pela Chefe da Divisão de Governança, Apoio à Gestão de TIC e Iniciativas Nacionais, apresentando as alterações no anexo III, 5.4 a 5.6, da Portaria GP n.º 0436, de 13/5/2021, bem como aquelas de natureza técnica e revisionais de praxe, doc. 48 do Proad 2070/2021;
CONSIDERANDO os despachos presidenciais, docs. 49 e 50 do referido proad,

RESOLVE

CAPÍTULO I
DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Art. 1º. Estabelecer a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 14ª Região, da qual são parte integrante todas as normas e procedimentos complementares e afins editados pelo Tribunal e que tem como objetivo garantir um ambiente tecnológico controlado e seguro de forma a oferecer todas as informações necessárias aos processos deste Tribunal, com integridade, confidencialidade e disponibilidade.
Parágrafo único. A presente Política de Segurança da Informação tem por fundamento as seguintes referências legais e normativas:

I - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação no âmbito da Administração Pública Federal;
II - Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;
III - Resolução nº 370, de 28 de janeiro de 2021, do Conselho Nacional de Justiça, Estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
IV - Norma ABNT NBR ISO/IEC 27001:2022, que normatiza o Sistema de Gestão da Segurança da Informação;
V - Norma ABNT NBR ISO/IEC 27002:2022, que normatiza o Código de Prática para Controles da Segurança da Informação;
VI - Código Penal Brasileiro;
VII - Lei 8.112/90, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;
VIII - Decreto nº 10.222, de 05 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;
IX - ISO/IEC 27003:2020, que define uma visão geral sobre sistemas de gestão de segurança da informação e de termos e conceitos utilizados;
X - Lei 13.709 - Lei Geral de Proteção de Dados pessoais (LGPD);
XI - Estratégia Nacional de Segurança Cibernética do Poder Judiciário - ENSEC-PJ (Res CNJ 396/2021);
XII - Portaria CNJ 162/2021 - Aprova Protocolos e Manuais criados pela Resolução nº 396/2021.
Art. 2º. Para os efeitos deste Ato aplicam-se as seguintes definições:
I - Auditoria: processo sistemático, independente e documentado para obter evidências de auditoria e avaliá-las objetivamente para determinar em que medida os critérios de auditoria são atendidos;
II - Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;
III - Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
IV - Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
V - Dispositivos Móveis: equipamentos portáteis com capacidade computacional de processamento, tais como notebooks, smartphones, tablets, entre outros;
VI - Integridade: propriedade de precisão e completude;
VII - Plano de Continuidade da Prestação dos Serviços: conjunto de ações de prevenção e procedimentos de recuperação a serem seguidos para proteger os processos críticos de trabalho contra efeitos de falhas de equipamentos, acidentes, ações intencionais ou desastres naturais significativos, assegurando a disponibilidade das informações.
VIII - Recurso de Tecnologia da Informação: qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação, instalações físicas que os abriguem.
IX - Segurança da Informação: conjunto de ações, controles e medidas para assegurar a preservação da confidencialidade, disponibilidade e integridade da informação.
X - Trabalho Remoto: Modalidade de trabalho realizada de forma remota, com a utilização de recursos tecnológicos próprios ou do Tribunal.
XI - Usuários: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores, aposentados, estagiários, e outras pessoas que se encontrem a serviço da Justiça do Trabalho, utilizando, mesmo que em caráter temporário, os recursos tecnológicos do TRT da 14ª Região.
Art. 3º. As disposições desta Resolução aplicam-se a todos os usuários de ativos de informação institucionais, tais como: magistrados; servidores ocupantes de cargo efetivo ou em comissão, requisitados ou cedidos; advogados; jurisdicionados; empregados de empresa prestadora de serviços terceirizados; consultores; estagiários; e visitantes.
§1º Os contratos, convênios e instrumentos congêneres firmados pelo Tribunal que envolvam o acesso ou a custódia de ativos de informação institucionais por parte das contratadas, conveniadas ou congêneres, incluindo a utilização de recursos de tecnologia da informação e comunicação, deverão conter cláusula exigindo a observância desta Resolução.
§2º Para contratações e acordos deverão ser considerados os seguintes requisitos mínimos:
a avaliação de segurança relacionada aos fornecedores anteriormente ao pacto firmado, considerando as práticas de segurança da informação;
a inclusão de cláusulas contratuais específicas de segurança da informação, atribuindo responsabilidades e requisitos mínimos; e
o monitoramento e controle da publicidade de artefatos gerados que sejam considerados sigilosos.
§3º Os fornecedores de produtos ou serviços, ao tratarem os dados pessoais a eles confiados pelo Tribunal, serão considerados Operadores e deverão aderir à Política de Privacidade e Proteção de Dados Pessoais deste Tribunal, além de cumprir os deveres legais e contratuais respectivos.

CAPÍTULO II
DA UTILIZAÇÃO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

Art. 4º. O uso adequado dos recursos de Tecnologia da Informação visa garantir a continuidade da prestação jurisdicional deste Tribunal.
Parágrafo único. Os recursos de Tecnologia da Informação pertencentes ao Tribunal Regional do Trabalho da 14ª Região e disponíveis para os usuários serão utilizados em atividades relacionadas às suas funções institucionais.
Art. 5º. A utilização dos recursos de tecnologia da informação e comunicação é passível de monitoramento e controle por parte deste Tribunal, respeitando, em todo caso, os preceitos da Lei Geral de Proteção de Dados, fornecendo evidências nos casos de incidentes de segurança.
§1º O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
§2º Serão realizadas auditorias ordinárias periódicas, cujos relatórios serão encaminhados ao Comitê de Segurança da Informação.
§3º As auditorias extraordinárias serão realizadas com o intuito de apurar eventos que deponham contra a segurança e as boas práticas no uso dos recursos de Tecnologia da Informação.

CAPÍTULO III
DA PROPRIEDADE DA INFORMAÇÃO

Art. 6º. Os documentos, processos, tecnologias e demais ativos de informação produzidos pelos usuários no exercício de suas funções institucionais são propriedade do Tribunal, independentemente da forma de sua apresentação ou armazenamento, e deverão ser utilizados exclusivamente para fins relacionados às atividades institucionais.
§ 1º O acesso e manuseio dos recursos de tecnologia de informação e comunicação deverão ser controlados e estar de acordo com esta Política, bem como demais normativos e procedimentos aprovados no âmbito do Tribunal.
§ 2º Quando os documentos, processos, tecnologias e demais ativos de informação forem produzidos por terceiros para uso exclusivo do Tribunal, ficam os seus criadores obrigados ao sigilo permanente a respeito de tais produtos, sendo vedada a sua veiculação e reutilização em projetos para outrem, salvo se expressamente autorizado por este Tribunal.

CAPÍTULO IV

DAS INFORMAÇÕES GERADAS NO TRIBUNAL

Art. 7º. Toda informação gerada no Tribunal será classificada em termos de seu valor, requisitos legais, sensibilidade, criticidade e necessidade de compartilhamento.

§ 1º A nomeação dos gestores da informação, responsáveis por essa classificação, a definição dos procedimentos e o termo de responsabilidade e compromisso serão definidos pelo Comitê de de Segurança da Informação (CSI), mediante aprovação da Presidência do Tribunal.

§ 2º O usuário dos ativos de informação assume o compromisso de não utilizar, revelar ou divulgar a terceiros, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação classificada como sigilosa que tenha ou venha a ter conhecimento em razão de suas funções na instituição, enquanto durar o prazo de restrição do seu acesso à informação.

§ 3º O Tribunal deverá adotar recursos para proteção da informação adequados e proporcionais ao seu grau de confidencialidade e criticidade, independentemente do suporte em que resida ou da forma pela qual seja veiculada, e que sejam capazes de assegurar a sua autenticidade, integridade e disponibilidade.

§4° O Tribunal providenciará dispositivos de proteção proporcionais ao grau de confidencialidade e de criticidade da informação, independentemente do suporte em que resida ou da forma pela qual seja veiculada, capazes de assegurar a sua autenticidade, integridade e disponibilidade.

Art. 8º. As informações, sistemas e métodos gerados ou criados pelos usuários, no exercício de suas funções, independentemente da forma de sua apresentação ou armazenamento, são propriedade do Tribunal e serão utilizadas exclusivamente para fins relacionados às atividades específicas.

Parágrafo único. Quando as informações, sistemas e métodos forem gerados ou criados por terceiros para uso exclusivo do Tribunal, ficam os criadores obrigados ao sigilo permanente de tais produtos, sendo vedada a sua reutilização em projetos para outrem.

CAPÍTULO V

DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO

Art. 9º. Compete à alta administração do Tribunal realizar a gestão estratégica da segurança da informação, por intermédio do Comitê de Segurança da Informação (CSI), que será composto por determinação da Presidência, conforme Anexo I desta Política.

Art. 10. As competências do Comitê de Segurança da Informação e seu funcionamento, são regulados no Anexo I desta Política.

Art. 11. Incumbe à chefia imediata e superior do usuário verificar a observância da Política de Segurança da Informação no âmbito de sua unidade, comunicando, de imediato, ao Comitê de Segurança da Informação, as irregularidades constatadas, para as providências cabíveis.

CAPÍTULO V

DO SUBCOMITÊ DE CRISES CIBERNÉTICAS

Art. 12. O Subcomitê de Crises Cibernéticas será composto conforme Anexo I desta Política.

Art. 13. As competências do Subcomitê de Crises Cibernéticas e seu funcionamento, são regulados no Anexo I desta Política.

CAPÍTULO VI

DO USO DE DISPOSITIVOS MÓVEIS

Art. 14. O uso de dispositivos móveis será regulamentado em norma complementar, com diretrizes específicas e procedimentos próprios, considerando as seguintes diretrizes gerais:

I - O uso de dispositivos móveis por usuários nas dependências do TRT14 somente será realizado para os interesses de negócio da instituição.

II - À exceção dos casos previstos em contratos firmados com o TRT14, ao visitante não é permitido o uso de dispositivo móvel particular para acessar à rede do TRT14.

III - os dispositivos móveis que não são de propriedade do TRT14 não poderão fazer uso da rede corporativa, permitido somente o acesso à internet, por meio de rede específica para visitante ou autorização expressa pela unidade competente;

IV - a concessão de uso deve estar vinculada à concordância do usuário às normas internas de uso deste serviço, seguindo os critérios estabelecidos pelo TRT14, podendo a permissão de uso ser revogada, sem prévio aviso, caso seja identificada alguma não conformidade com as regras de segurança da informação e comunicações estabelecidas pelo TRT14.

Parágrafo único. É recomendada a adoção de mecanismos que garantam a proteção e sigilo dos dados e informações classificadas armazenados nos dispositivos móveis.

CAPÍTULO VII

DA SEGURANÇA DA INFORMAÇÃO NO TRABALHO REMOTO

Art. 15. A Segurança da Informação no trabalho remoto será regulamentada em norma complementar, com diretrizes específicas e procedimentos próprios, considerando as seguintes diretrizes gerais:

I - o acesso remoto deve ser concedido estritamente por necessidade funcional justificada, exigindo a utilização de equipamento de comunicação apropriado, que esteja com os níveis adequados de proteção, incluindo métodos de acesso remoto seguro;

II - medidas que apoiam a segurança da informação devem ser implementadas para proteger as informações em trânsito, acessadas, processadas ou armazenadas em locais de trabalho remoto;

III - O local utilizado para a realização do teletrabalho ou trabalho remoto deve ser adequado às condições de privacidade e segurança necessárias ao serviço, zelando pelo princípio da confidencialidade;

IV - preservar o sigilo dos dados acessados de forma remota, mediante observância das normas internas de segurança da informação e da comunicação, bem como manter atualizados os sistemas institucionais instalados nos equipamentos de trabalho.

CAPÍTULO VIII

DAS NORMAS COMPLEMENTARES

Art. 16. As normas complementares, que derivam desta Política de Segurança da Informação principal, especificam obrigações a serem seguidas pelos usuários, regras e procedimentos em nível gerencial relacionados à gestão da segurança da informação, definindo suas diretrizes, abarcando os seguintes temas anexo a este documento:

I - NSI01 – Comitê de Segurança da Informação e Subcomitê de Crises Cibernéticas, conforme Anexo I desta política;

II - NSI02 – Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação - ETIR, conforme Anexo II desta política;

III - NSI03 – Política de Uso de Recursos de Tecnologia da Informação e Comunicação e Controle de Acesso, conforme Anexo III desta política;

IV - NSI04 – Gestão de Incidentes de Segurança da Informação, conforme Anexo IV desta política;

V - NSI05 – Gestão de Riscos de Tecnologia da Informação e Comunicações, conforme Anexo V desta política;

VI - NSI06 – Plano de Continuidade dos Serviços Essenciais de TIC, conforme Anexo VI desta política;

Art. 17. Poderão ser criadas normas complementares e procedimentos, sem prejuízo dos normativos indicados no artigo anterior, sobre outros temas relacionados à Segurança da Informação e conforme necessidade e conveniência, desde que aprovadas pelo Comitê de Segurança da Informação.

CAPÍTULO IX

DAS DISPOSIÇÕES GERAIS E TRANSITÓRIAS

Art. 18. O descumprimento das normas referentes à Política de Segurança da Informação deste Tribunal poderá acarretar, isolada ou cumulativamente, nos termos da legislação vigente, sanções administrativas, civis e penais.

Art. 19. As normas complementares às diretrizes gerais definidas na Política de Segurança da Informação deste Tribunal serão editadas sob a forma de anexos, que integrarão a presente Portaria.
Parágrafo único. A Política de Segurança da Informação será revista anualmente, de preferência no primeiro semestre ou quando necessário, em menor prazo.

Art. 20. Revogar os efeitos da Portaria GP n.º 0436, de 13/5/2021;
Art. 21. O presente Ato entra em vigor a partir da data de sua publicação.
Publique-se.
(assinado eletronicamente)
OSMAR J. BARNEZE
Desembargador-Presidente

Anexos
Anexo 1: Download
Anexo 2: Download
Anexo 3: Download
Anexo 4: Download
Anexo 5: Download
Anexo 6: Download

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO
Gabinete da Presidência

PORTARIA GP N.º 0581, DE 29 DE MAIO DE 2024.

ANEXO I

NSI01 – Comitê de Segurança da Informação e

Subcomitê de Crises Cibernéticas

1. DO OBJETO

1.1 Esta Norma dispõe sobre o Comitê de Segurança da Informação (CSI) e institui o Subcomitê de Crises Cibernéticas (SCC).

2. DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO (CSI)

2.1 O CSI terá a seguinte composição:

I. O(A) Coordenador(a) do Comitê de Governança de TIC;
II. 01 (um(a)) Desembargador(a) do Trabalho, nomeado(a) através de portaria específica da Presidência do TRT da 14ª Região.
III. Juiz(a) Auxiliar da Presidência;
IV. Juiz(a) Auxiliar da Corregedoria;
V. Secretário(a) de Governança e Gestão Estratégica;
VI. Diretor(a)-Geral;
VII. Secretário(a)-Geral da Presidência;
VIII. Secretário(a)-Geral Judiciário(a);
IX. Secretário(a) de TIC;
X. Chefe da Divisão de Segurança da Informação da SETIC.
XI. Coordenador(a) de Infraestrutura e Serviços da SETIC;

2.2 Fica definido o(a) Coordenador(a) do Comitê de Governança de TIC como o(a) Coordenador(a) deste comitê e o(a) Desembargador(a) do Trabalho como vice-coordenador(a) (suplente).
2.3 O Comitê poderá convocar representantes de unidades do Tribunal ou outras partes interessadas para participar das reuniões, se necessário.

2.4 Das Atribuições

2.4.1 Cabe ao CSI:
I. Elaborar e submeter à Presidência do Tribunal, ouvido o Comitê de Governança de Tecnologia da Informação e Comunicações, propostas de normas e políticas de uso dos recursos de informação;
II. Rever a Política de Segurança da Informação e normas relacionadas e sugerir alterações;

III. Estabelecer diretrizes e definições estratégicas para as ações e projetos relacionados à Segurança da Informação;
IV. Dirimir dúvidas e deliberar sobre questões não contempladas na Política de Segurança da Informação e em normas relacionadas;
V. Propor e acompanhar planos de ação para aplicação da Política de Segurança da Informação, assim como campanhas de conscientização dos usuários;
VI. Receber comunicações de descumprimento das normas referentes à Política de Segurança da Informação deste Tribunal, instruí-las com os elementos necessários à sua análise e apresentar parecer ao órgão ou autoridade competente a apreciá-las;
VII. Solicitar à Divisão de Segurança da Informação, quando necessário, a realização de auditorias extraordinárias, acerca do uso dos recursos de tecnologia da informação do Tribunal;
VIII. Avaliar relatórios e resultados de auditorias apresentados pela Divisão de Segurança da Informação;
IX. Assessorar a alta administração do Tribunal em todas as questões relacionadas à segurança da informação.

2.4.2 Cabe ao(à) coordenador(a) do CSI:

I. convocar ou fazer convocar reuniões ordinárias e extraordinárias;
II. comparecer a todas as reuniões, pessoalmente ou representado pelo vice-coordenador;
III. estabelecer e fazer cumprir o cronograma de atividades;
IV. zelar pela eficiência do colegiado;
V. mediar conflitos no âmbito do colegiado;
VI. imprimir celeridade aos processos de deliberação; e
VII. assinar as atas de reunião.

2.4.3 Da Unidade de Apoio Executivo (UAE)

2.5.3.1 A Secretaria de Tecnologia da Informação e Comunicação realizará a gestão administrativa do CSI e cuidará de aspectos relativos à organização, comunicação e transparência do colegiado.

2.4.3.2 Cabe à UAE:

I - receber, organizar e registrar em pauta os assuntos a serem debatidos nas reuniões;
II - enviar aos membros do colegiado as pautas e demais documentos necessários à realização da reunião;
III - convidar os membros para reuniões convocadas pelo coordenador ou por 1/3 (um terço) dos membros do colegiado;
IV - providenciar os recursos físicos e tecnológicos para as reuniões;
V - redigir as atas das reuniões e colher a assinatura do coordenador;
VI - fazer publicar as atas das reuniões e demais documentos, exceto quando contiverem informação total ou parcialmente sigilosa, hipótese em que se publicará certidão, extrato ou cópia com ocultação da parte sob sigilo;
VII - monitorar o conteúdo e a vigência dos atos normativos referentes ao colegiado; e
VIII - providenciar e fornecer informações a respeito do colegiado, quando requeridas por parte interessada.

2.4.3.3 Cabe ao(à) titular da UAE:

I - zelar pelo cumprimento das atribuições estabelecidas no item 2.4.3.2;

II - manter atualizadas as informações do colegiado no sítio eletrônico do Tribunal, inclusive no que diz respeito ao conteúdo e à vigência dos atos normativos;

III - dar ciência ao coordenador do colegiado sobre eventual inobservância da periodicidade de realização das reuniões ordinárias;

IV - reportar ao coordenador as ocorrências que possam dificultar, direta ou indiretamente, a realização de reuniões e/ou a divulgação dos documentos produzidos pelo colegiado; e

V - reportar à Presidência do Tribunal as ocorrências a que faz referência o inciso IV deste parágrafo, em caso de omissão do coordenador.

2.5.3. As atribuições mencionadas no item 2.4.3.3 poderão ser delegadas pelo titular da UAE a servidor(a) a ele(a) subordinado(a).

2.5 Das Reuniões

2.5.1 O CSI se reunirá, ordinariamente, a cada 03 (três) meses ou, extraordinariamente, quando necessário.

2.5.2 As reuniões ordinárias ocorrerão em datas definidas pelo coordenador do colegiado, observadas a periodicidade definida no caput deste artigo e a antecedência mínima de 5 (cinco) dias para a convocação.

2.5.3 As reuniões do colegiado temático serão presenciais, telepresenciais ou híbridas.

2.5.4 A convocação para as reuniões se dará por qualquer meio admitido em direito, dispensada a antecedência mínima no caso de reunião extraordinária.

2.5.5 Se ocorrerem duas ou mais reuniões num mesmo mês, faculta-se ao colegiado, com a concordância de seu coordenador, proceder à publicação de ata mensal única, com o registro dos fatos ocorridos nas reuniões havidas no período.

2.5.6 O colegiado poderá convidar, para participar como colaboradores, sem direito a voto, representantes de órgãos ou de unidades organizacionais do Tribunal e profissionais de outras instituições com conhecimentos relacionados às áreas de atuação deste comitê.

2.6 Das Pautas e Atas de Reunião

2.6.1 As atas conterão, no mínimo, as seguintes informações:

I - a data, o horário e o local da reunião;

II - o breve relato das manifestações ocorridas durante a reunião;

III - as deliberações tomadas;

IV - o responsável pelo cumprimento de cada deliberação; e

V - os nomes dos participantes.

2.6.2 As pautas poderão integrar o conteúdo das atas de reunião, em vez de serem apresentadas em documento à parte.

2.6.3 As pautas e as atas serão juntadas ao processo administrativo eletrônico respectivo em até 15 (quinze) dias depois de realizada a reunião.

2.6.4 Cabe à UAE diligenciar para que o prazo estabelecido no item 2.6.3 seja atendido.

2.6.5 Do Quórum de Reunião e Quórum de Votação

2.6.5.1 Para instalar-se reunião do CSI, será exigido o quorum de ⅓ (um terço) dos membros, presente, necessariamente, o coordenador.

2.6.5.2 As deliberações do colegiado serão tomadas por maioria simples, considerando o número de membros presentes na reunião.

2.6.5.3 Todos os membros do colegiado terão voto de igual peso.
2.6.5.4 Cabe ao coordenador, em caso de empate, o voto de qualidade.

3. DO SUBCOMITÊ DE CRISES CIBERNÉTICAS - SCC

3.1 O SCC será composto pelos integrantes do CSI e ainda:

I. Secretário(a) de Comunicação Social e Eventos Institucionais;
II. Secretário(a) de Orçamento e Finanças;
III. Chefe da Divisão de Governança, Apoio à Gestão de TIC e Iniciativas Nacionais da SETIC;
IV. Coordenador(a) de Desenvolvimento de Soluções e Aplicações da SETIC;
V. Chefe do Núcleo de Segurança Institucional.

3.2 O(A) atual Coordenador(a) do CSI coordenará o Subcomitê e terá como subcoordenador(a) o(a) Chefe da Divisão de Segurança da Informação.
3.3 O Subcomitê poderá convocar representantes de unidades do Tribunal ou outras partes interessadas para participar das reuniões, se necessário.

3.4 Das Atribuições

3.4.1 Cabe ao SCC:

I. Reunir-se com a Equipe de Tratamento e Resposta a Incidentes Cibernéticos na sala de situação, providenciada e padronizada nos termos do anexo II da Portaria CNJ Nº 162, de 10 de Junho de 2021;
II. Comunicar os incidentes graves ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ);
III. Realizar a análise criteriosa das ações tomadas, observando as que foram bem-sucedidas e as que ocorreram de forma inadequada;
IV. Gerenciar e deliberar sobre as ações necessárias para o tratamento de crises cibernéticas.

3.4.2 Cabe ao coordenador do SCC:

I. convocar ou fazer convocar reuniões ordinárias e extraordinárias;
II. comparecer a todas as reuniões, pessoalmente ou representado pelo vice-coordenador;
III. estabelecer e fazer cumprir o cronograma de atividades;
IV. zelar pela eficiência do colegiado;
V. mediar conflitos no âmbito do colegiado;
VI. imprimir celeridade aos processos de deliberação; e
VII. assinar as atas de reunião.

3.4.3 Da Unidade de Apoio Executivo (UAE)

3.4.3.1 A Secretaria de Tecnologia da Informação e Comunicação realizará a gestão administrativa do SCC e cuidará de aspectos relativos à organização, comunicação e transparência do colegiado.

3.4.3.2 Cabe à UAE:

I - receber, organizar e registrar em pauta os assuntos a serem debatidos nas reuniões;

II - enviar aos membros do colegiado as pautas e demais documentos necessários à realização da reunião;

III - convidar os membros para reuniões convocadas pelo coordenador ou por 1/3 (um terço) dos membros do colegiado;

IV - providenciar os recursos físicos e tecnológicos para as reuniões;

V - redigir as atas das reuniões e colher a assinatura do coordenador;

VI - fazer publicar as atas das reuniões e demais documentos, exceto quando contiverem informação total ou parcialmente sigilosa, hipótese em que se publicará certidão, extrato ou cópia com ocultação da parte sob sigilo;

VII - monitorar o conteúdo e a vigência dos atos normativos referentes ao colegiado; e

VIII - providenciar e fornecer informações a respeito do colegiado, quando requeridas por parte interessada.

3.4.3.3 Cabe ao titular da UAE:

I - zelar pelo cumprimento das atribuições estabelecidas no item 3.4.3.2;

II - manter atualizadas as informações do colegiado no sítio eletrônico do Tribunal, inclusive no que diz respeito ao conteúdo e à vigência dos atos normativos;

III - dar ciência ao coordenador do colegiado sobre eventual inobservância da periodicidade de realização das reuniões ordinárias;

IV - reportar ao coordenador as ocorrências que possam dificultar, direta ou indiretamente, a realização de reuniões e/ou a divulgação dos documentos produzidos pelo colegiado; e

V - reportar à Presidência do Tribunal as ocorrências a que faz referência o inciso IV deste parágrafo, em caso de omissão do coordenador.

3.4.3.4 As atribuições mencionadas no item 3.4.3.3 poderão ser delegadas pelo titular da UAE a servidor a ele subordinado.

3.4.4. Das Reuniões

3.4.4.1 O SCC se reunirá na sala de situação, assim que a ETIR identificar que um incidente constitui uma crise cibernética.

3.4.4.2 A sala de situação é o local a partir do qual são geridas as situações de crise, devendo dispor dos meios necessários e estar próxima a um local onde se possa fazer declarações públicas à imprensa e com o acesso restrito ao SCC e a outros atores eventualmente convidados a participar de reuniões.

3.4.4.3 O SCC se reunirá em sala de situação preparada com os meios necessários para a deliberação com tranquilidade a respeito do ambiente cibernético. A sala de situação deverá atender, preferencialmente, aos seguintes requisitos:

I. deve conter ao menos 1 (um) ramal telefônico;
II. capacidade para, pelo menos, 6 (seis) pessoas;
III. pontos de redes e notebooks para acesso à internet;
IV. deve conter equipamento com função de impressão e scanner;
V. deve conter fragmentadora de papel;
VI. deve ter acesso controlado;
VII. deve se localizar, preferencialmente, próximo a local onde se possa fazer declarações públicas à imprensa.

3.4.4.4 O SCC deve reunir-se presencialmente ou virtualmente, através de tecnologia oficial de videoconferência adotada no Tribunal, para deliberar se o incidente reportado pela ETIR constitui crise cibernética.

3.4.4.5 Quando for identificada como a maneira mais conveniente para a reunião intempestiva do SCC, será utilizada a solução de videoconferência implantada no Tribunal para as deliberações deste Subcomitê.

3.4.4.6 Caso seja confirmada a crise cibernética, o SCC entrará em estado de convocação permanente, podendo reunir-se a qualquer horário para discutir, deliberar e agir no tratamento da crise em curso.

3.4.4.7 Enquanto perdurar o incidente, a coordenação do SCC deverá convocar reuniões regulares para avaliar o progresso até que seja possível retornar à condição de normalidade.

3.4.4.8 O acesso às reuniões do SCC deve ser restrito aos membros deste Subcomitê e a atores eventualmente convidados a participar das reuniões.

3.4.4.9 O SCC deve ter acesso ágil a meios que permitam fazer declarações públicas à imprensa.

3.4.4.10 O SCC deve contar com equipe dedicada à execução de atividades administrativas necessárias durante o período de crise.

3.4.5 Das Pautas e Atas de Reunião

3.4.5.1 As atas conterão, no mínimo, as seguintes informações:

I - a data, o horário e o local da reunião;

II - o breve relato das manifestações ocorridas durante a reunião;

III - as deliberações tomadas;

IV - o responsável pelo cumprimento de cada deliberação; e

V - os nomes dos participantes.

3.4.5.2 As pautas poderão integrar o conteúdo das atas de reunião, em vez de serem apresentadas em documento à parte.

3.4.5.3 As pautas e as atas serão juntadas ao processo administrativo eletrônico respectivo em até 15 (quinze) dias depois de realizada a reunião.

3.4.5.4 Cabe à UAE diligenciar para que o prazo estabelecido no item 3.4.5.4 seja atendido.

3.4.6 Do Quórum de Reunião e Quórum de Votação

3.4.6.1 Para instalar-se reunião do SCC, será exigido o quorum de ⅓ (um terço) dos membros, presente, necessariamente, o coordenador.

3.4.6.2 As deliberações do colegiado serão tomadas por maioria simples, considerando o número de membros presentes na reunião.

3.4.6.3 Todos os membros do colegiado terão voto de igual peso.

3.4.6.4 Cabe ao coordenador, em caso de empate, o voto de qualidade.

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO
Gabinete da Presidência

PORTARIA GP N.º 0581, DE 29 DE MAIO DE 2024.

ANEXO II

NSI02 – Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação - ETIR

1. Objetivos

1.1. Estabelecer as diretrizes para o funcionamento da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR) do Tribunal Regional do Trabalho da 14ª Região.

2. Motivações

2.1. Alinhamento às normas, regulamentações e melhores práticas relacionadas à Segurança da Informação.
2.2. Necessidade de formalização da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR) e seu funcionamento.
2.3. Proteção do ambiente tecnológico do Tribunal.

3. Conceitos e Definições

3.1. **Artefato malicioso:** é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;
3.2. **Comunidade ou Público Alvo:** é o conjunto de pessoas, setores, órgãos ou entidades atendidas pela Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação;
3.3. **Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação – ETIR:** Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança da informação.
3.4. **Incidente de segurança da informação:** Um único ou uma série de eventos indesejados ou inesperados de segurança da informação que têm uma probabilidade significativa de colocar em perigo as operações da instituição e ameaçar a segurança da informação.

3.5. **Tratamento de Incidentes de Segurança da Informação:** conjunto de processos para detectar, relatar, avaliar, responder, lidar e aprender com incidentes de segurança da informação.

3.6. **Vulnerabilidade:** fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças.

4. Referências normativas

4.1. Instrução Normativa GSI/PR nº 1, de 13.06.2008, do Gabinete de Segurança Institucional da Presidência da República, a qual disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências

4.2. Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14.08.2009, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais –ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta –APF.

4.3. Norma Complementar nº 08/IN01/DSIC/GSIPR, de 14.08.2010, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais –ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta –APF.

4.4. Norma Técnica ISO/IEC 27000:2018, que especifica conceitos e definições relacionados às normas de segurança da informação. (item incluído pela Portaria nº 4.786/2020).

4.5. Resolução CNJ n. 370, de 28 de janeiro de 2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) e estabelece as diretrizes para sua governança, gestão e infraestrutura.

4.6. Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais.

4.7. Portaria CNJ n. 242 de 10 de novembro de 2020, que institui o Comitê de Segurança Cibernética do Poder Judiciário.

5. Missão da ETIR

5.1. Prover capacidade adequada para resposta e tratamento de incidentes de segurança da informação em ambiente tecnológico.

6. Público-alvo

6.1. O público-alvo da ETIR é formado por todos os usuários do ambiente tecnológico deste Tribunal.

6.2. A ETIR relaciona-se, internamente, com as diversas unidades da Secretaria de Tecnologia da Informação e Comunicação e com o Comitê de Segurança da Informação.

6.3. Externamente, a ETIR se relaciona com o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil – Cert.br e outros órgãos do Poder Judiciário Federal.

7. Modelo de Implementação

7.1. A ETIR será composta por servidores da Secretaria de Tecnologia da Informação e Comunicação, que, além de suas funções regulares, desempenharão as atividades relacionadas ao tratamento e à resposta a incidentes de segurança da informação.

8. Estrutura Organizacional e Composição

8.1. A ETIR é subordinada à Secretaria de Tecnologia da Informação e Comunicação e é coordenada pela Divisão de Segurança da Informação.

8.2. A ETIR é composta por servidores da Secretaria de Tecnologia da Informação e Comunicação, sendo:

- Chefe e Servidores da Divisão de Segurança da Informação;
- Chefe da Seção de Gerência de Redes e Comunicação;
- Chefe da Seção de Suporte;
- Chefe da Seção de Infraestrutura Computacional;
- Chefe da Coordenadoria de Infraestrutura e Serviços;
- Chefe da Coordenadoria de Desenvolvimento de Soluções e Aplicações.

8.3. Caso necessário, deverão ser convocados outros servidores da Secretaria de Tecnologia da Informação e Comunicação e/ou servidores de outras áreas do Tribunal (jurídica, gestão de pessoas, comunicação social, etc.) para auxiliar a equipe no desenvolvimento de suas atividades.

9. Autonomia

9.1. A autonomia da ETIR é compartilhada. A equipe recomendará, no mínimo, aos chefes das áreas técnicas envolvidas e ao Secretário da Secretaria de Tecnologia da Informação e Comunicação, os procedimentos a serem executados ou as medidas de recuperação durante um incidente e apresentará as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas). De acordo com a gravidade do incidente, a proposição deverá, ainda, ser submetida ao Comitê de Segurança da Informação e/ou à Presidência do Tribunal. As ações serão sempre definidas em conjunto com as instâncias consultadas.

10. Serviços prestados pela ETIR

10.1. Tratamento de Incidentes de Segurança da Informação: serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

10.2. Tratamento de Artefatos Maliciosos: serviço que consiste em receber informações ou cópia de artefato malicioso que foi utilizado no ataque, ou em qualquer atividade desautorizada ou maliciosa. Uma vez recebido, o mesmo deve ser analisado, ou seja, deve-se buscar a natureza do artefato, seu mecanismo, versão e objetivo, para que seja desenvolvida, ou pelo menos sugerida, uma estratégia de detecção, remoção e defesa.

10.3. Tratamento de Vulnerabilidades: serviço que consiste em receber informações sobre vulnerabilidades, quer sejam em hardware ou software, objetivando analisar sua natureza, mecanismo e suas consequências e desenvolver estratégias para detecção e correção.

10.4. Emissão de alertas e advertências: serviço que consiste em divulgar alertas ou advertências imediatas como uma reação diante de um incidente de segurança em redes de computadores, com o objetivo de advertir a comunidade ou dar orientações sobre como a comunidade deve agir diante do problema.

10.5. Assim que identificar que um incidente constitui crise cibernética, reunir-se imediatamente com o Subcomitê de Crises Cibernéticas, prestando auxílio para suas deliberações.

11. Canal de comunicação de incidentes de segurança

11.1. A comunicação de incidentes cibernéticos suspeitos ou confirmados para a equipe deve ser realizada por e-mail, para o endereço etir@trt14.jus.br

12. Atualização da Norma

12.1. Esta norma será atualizada em conjunto com a revisão da Política de Segurança da Informação ou a qualquer tempo, quando assim recomendado pelo Comitê de Segurança da Informação.

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO
Gabinete da Presidência

PORTARIA GP N.º 0581, DE 29 DE MAIO DE 2024.

ANEXO III

NSI03 – Política de Uso de Recursos de Tecnologia da Informação e Comunicação e Controle de Acesso

1. Objetivos

1.1. Estabelecer a Política de Uso de Recursos de Tecnologia da Informação e Comunicação e Controle de Acesso no âmbito do Tribunal Regional do Trabalho da 14ª Região.

2. Motivações

2.1. Alinhamento às normas, regulamentações e melhores práticas relacionadas à matéria.

2.2. Necessidade de definição de diretrizes voltadas à gestão dos recursos de tecnologia da informação.

2.3. Promover a segurança e continuidade das atividades do TRT da 14ª Região.

3. Referências normativas

3.1. Portaria GP 0436, de 13 de maio de 2021, do TRT da 14ª Região, que institui a Política de Segurança da Informação e Comunicação no âmbito do TRT da 14ª Região.

3.2. Norma Técnica ISO/IEC 27000:2018, que especifica conceitos e definições relacionados à segurança da informação.

3.3. Norma Técnica 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 do contexto da organização.

3.4. Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação.

3.5. Resolução CSJT nº 164, de 18 de março de 2016, que disciplina o uso e a concessão de certificados digitais institucionais no âmbito da Justiça do Trabalho de primeiro e segundo graus.

3.6. Lei 13.709 de 14 de agosto de 2018 (LGPD), que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado.

4. Conceitos e definições

4.1. Usuários: magistrados e servidores do quadro efetivo em atividade, servidores cedidos ou requisitados de outros órgãos e ocupantes de cargo em comissão;

4.2. Rede corporativa: conjunto de redes de dados locais e de longa distância (LAN/WAN), logicamente integradas, que oferecem serviços de comunicação interna de dados (intranet) e externa (internet) ao TRT da 14ª Região;

4.3. Certificado Digital A3: documento de identificação eletrônica, armazenado em mídia criptográfica (token), emitido por autoridade certificadora, que permite a identificação segura dos usuários no meio digital;

4.4. Recursos de TIC: impressoras, scanners, multifuncionais, computadores desktops computadores notebooks, servidores de rede, equipamentos de rede (switches, access points, roteadores, modems), equipamentos de infraestrutura de data center (storage, servidores Blade, appliance de segurança), sistemas informatizados, softwares, serviços de comunicação (internet e intranet) etc;

4.5. Ambiente Computacional: conjunto de hardware e software destinado ao processamento de dados.

4.6. SAU - Sistema de Atendimento ao Usuário: ferramenta de gestão dos serviços de atendimento prestados pela SETIC. Registra requisições ou incidentes oriundas dos usuários dos recursos de TIC.

4.7. Segurança da Informação: conjunto de regras que objetivam garantir a confidencialidade, integridade, disponibilidade e integridade da informação gerada.

5. Das contas de usuários

5.1. A Secretaria de Tecnologia da Informação e Comunicação (SETIC) realizará a habilitação inicial dos usuários para acesso à rede corporativa. A senha de acesso é de uso pessoal e intransferível, cabendo aos usuários mantê-la em sigilo, sendo vedada a sua cessão ou empréstimo sob qualquer pretexto.

5.2. A solicitação de habilitação inicial à rede corporativa deverá ser realizada mediante abertura de chamado técnico no Sistema de Atendimento ao Usuário (SAU) da SETIC e pode ser feito pela unidade de Recursos Humanos, quando do ingresso de novo magistrado/servidor, ou responsável pela unidade organizacional onde o usuário está lotado.

5.3. A senha de acesso inicial deverá ser alterada pelo usuário, conforme política de senha definida pela SETIC, no momento em que for realizado seu primeiro acesso ou sempre que solicitado pelo sistema.

5.4. Incumbe ao gestor da unidade ou à chefia imediata a conferência regular dos acessos concedidos aos servidores e estagiários vinculados a sua unidade, e sempre que possível, realizar os ajustes ativando ou desativando as permissões aos sistemas utilizados e, caso necessário, solicitar à SETIC mediante abertura de chamado técnico:

5.4.1. concessão dos acessos necessários ao desenvolvimento das atividades dos servidores e estagiários vinculados a sua unidade;

5.4.2. a alteração dos níveis de acesso ou a remoção do acesso a sistemas concedidos a servidor ou estagiário da unidade, sempre que necessária sua adequação às atividades desenvolvidas;

5.4.3. a remoção dos acessos concedidos ao servidor ou estagiário, imediatamente após o afastamento ou desligamento da unidade;

5.5. Não solicitada a alteração ou exclusão no momento oportuno, a chefia poderá ser responsabilizada pelo acesso indevido do servidor/estagiário que não faça mais parte de sua unidade.

5.6. A Secretaria de Gestão de Pessoas (SGEP), no âmbito de suas competências, comunicará à SETIC, mediante abertura de chamado técnico no SAU, os casos de falecimento, exoneração, demissão, redistribuição, aposentadoria, remoção e cessão a outro órgão, retorno à origem ou término do estágio de estudantes, ou ainda sempre que um usuário for desligado da instituição, para remoção de todos os acessos concedidos.

5.7. Os atos decorrentes da utilização dos sistemas informatizados, por meio de conta de acesso com identificação e senha, são de responsabilidade do usuário a qual a conta está formalmente vinculada.

5.8. Visando evitar acessos indevidos aos sistemas e serviços institucionais de TIC, os usuários devem:

5.8.1. Após o término das atividades realizadas na estação de trabalho, efetuar o encerramento da seção (*logoff*) ou o bloqueio da tela por senha;

5.8.2. Sempre que ausentar-se de sua estação de trabalho, realizar o bloqueio da tela por senha.

5.9. A SETIC implantará políticas para criação, renovação, bloqueio e expiração de senhas, com o intuito de aumentar o nível de segurança da rede corporativa.

5.10. Os usuários poderão ser responsabilizados, de forma irrefutável, pelo uso inadequado dos sistemas informatizados a partir de acessos realizados com suas credenciais.

5.11. O privilégio de usuário administrador para os computadores somente será concedido aos servidores da SETIC que necessitarem de acesso privilegiado para o estrito desempenho das suas atividades funcionais.

5.12. Os direitos de acesso à rede corporativa, à *internet* e aos sistemas informatizados, serão concedidos aos magistrados, servidores do quadro efetivo, servidores cedidos ou requisitados de outros órgãos, ocupantes de cargo em comissão e estagiários que estejam, necessariamente, desempenhando suas atividades laborais no TRT da 14ª Região de acordo com a necessidade de cada unidade judiciária ou administrativa e de acordo com a atribuição referente ao cargo,

mediante deferimento de perfis e níveis de acessos aprovados pelo Comitê de Segurança da Informação.

5.13. Os direitos de acesso a cada recurso serão configurados pela SETIC, devendo ser observadas as necessidades do serviço e poderão ser retirados ou restringidos por solicitação de magistrado, responsável pela unidade lotacional ou ainda, de forma imediata, pela SETIC, sempre que for comprovadamente identificado o uso inadequado dos recursos de TIC em situações que possam colocar em risco a segurança da rede corporativa.

5.14. O processo de Gestão de Usuários de sistemas informatizados deverá ser instituído com o objetivo principal de implementar boas práticas de segurança da informação na gestão de identidades e credenciais eletrônicas, bem como para o controle de acessos e privilégios aos sistemas, serviços de TIC e equipamentos de tecnologia da informação. O processo deverá contemplar os seguintes subprocessos: I - Gerenciamento de identidades; II - Gerenciamento de acessos; e III - Gerenciamento de privilégios.

5.15. Com o objetivo de uniformizar e garantir a experiência única de interação com os sistemas institucionais, o processo de Gestão de Usuários de sistemas informatizados deverá, quando tecnicamente viável, adotar um padrão para utilização de credenciais de login único e interface de interação dos sistemas.

6. Do certificado digital

6.1. Aos usuários que justificarem a necessidade, será fornecido, pela Secretaria de Gestão de Pessoas, um certificado digital A3 com validade de 3 (três) anos.

6.2. O certificado digital é de uso pessoal, intransferível e hábil a produzir efeitos legais em todos os atos nos quais vier a ser utilizado, nos termos da legislação em vigor;

6.3. A utilização do certificado digital para qualquer operação implicará não repúdio e impedirá o titular de negar a autoria da operação ou de alegar que ela tenha sido praticada por terceiro;

6.4. O processo de emissão do certificado digital é composto pelas etapas de solicitação, validação presencial e gravação do certificado digital em mídia apropriada;

6.5. A renovação do certificado digital deverá ser realizada dentro do prazo de validade do certificado digital, em período não superior a 30 dias da data de expiração do certificado.

6.6. Os usuários deverão atentar-se para o prazo de expiração dos seus certificados, realizando processo de solicitação de novo certificado ou renovação dentro do prazo mencionado no parágrafo anterior.

6.7. O titular do certificado digital deverá custear a emissão de novo certificado ou ressarcir o erário em quaisquer das hipóteses abaixo:

6.7.1. Não renovação do certificado digital dentro do seu prazo de validade;

6.7.2. Renovação do certificado digital em desconformidade com o item 6, pelo valor proporcional ao tempo restante de validade do certificado;

6.7.3. Perda, extravio ou dano da mídia que resulte na inoperância do certificado digital, pelo valor proporcional ao tempo restante de validade do certificado;

6.7.4. Inutilização do certificado digital em razão de esquecimento da senha de utilização.

6.8. Para os demais casos, será observada a Resolução CSJT N. 164, de 18 de março de 2016, e suas eventuais alterações.

7. Do uso de criptografia e assinatura eletrônica

7.1. A criptografia de dados sensíveis será utilizada durante sua transmissão e armazenamento.

7.2. Os algoritmos de criptografia considerados seguros e utilizados pelo Tribunal serão os recomendados pelos órgãos reguladores e as melhores práticas da indústria, tais como AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography), entre outros, de acordo com a necessidade e o contexto de cada aplicação.

7.3. Os dados armazenados em equipamentos portáteis, servidores e bancos de dados, sempre que possível, deverão ser criptografados para proteger contra acessos não autorizados.

7.4. O uso de assinatura eletrônica será utilizado para garantir a integridade e autenticidade de documentos gerados e armazenados nos sistemas utilizados pelo Tribunal.

8. Do acesso à *internet*

8.1. O acesso à *internet* dar-se-á, exclusivamente, por intermédio dos meios autorizados e configurados pela SETIC.

8.2. Excetuando-se os casos previstos neste ato e nas demais políticas internas de segurança da informação do TRT14, o acesso à *internet* provido pela rede corporativa deverá se restringir às páginas com conteúdo estritamente relacionado com as atividades laborais.

8.3. Possuem direito de acesso à *internet*, através da rede corporativa, os magistrados e servidores do quadro efetivo em atividade, servidores cedidos ou requisitados de outros órgãos e ocupantes de cargo em comissão que estejam lotados nas unidades do TRT da 14ª Região.

8.3.1. Prestadores de serviços terceirizados e estagiários poderão ter acesso à *internet* durante o período de prestação dos serviços ou estágio, observando as disposições aqui enumeradas, desde que formalmente solicitado e justificado pelo responsável da unidade onde está sendo prestado o serviço terceirizado ou estágio.

8.4. Aos magistrados e servidores que comprovadamente necessitem de acesso a *internet* móvel, serão fornecidos dispositivos de acesso a

internet móvel (modem 4G), com limite de pacote de dados definido conforme condições contratuais.

8.4.1. Os acessos realizados a partir dos dispositivos de *internet* móvel estão restritos às atividades laborais e enquadrados nas regras desta portaria e demais regras relativas aos Recursos de TIC estabelecidas.

8.5. Constituem uso indevido dos serviços de acesso à *internet* as seguintes ações:

8.5.1. Acessar páginas de conteúdo considerado ofensivo, ilegal ou impróprio, tais como: violência, pornografia, racismo, jogos etc;

8.5.2. Utilizar programas de troca de mensagens em tempo real (bate-papo), exceto os definidos como ferramenta de trabalho e homologados pela SETIC;

8.5.3. Acessar páginas de áudio e vídeo em tempo real ou sob demanda, exceto nos casos de comprovada necessidade, mediante solicitação e liberação da SETIC;

8.5.4. Excluem-se da proibição do item 7.5.3 os serviços de videoconferência homologados pela SETIC que forneçam recursos de comunicação entre magistrados, servidores e órgãos, notadamente aqueles que dão suporte ao regime de trabalho remoto/teletrabalho.

8.5.5. Obter na *internet* arquivos (*download*) que não estejam relacionados com suas atividades funcionais, a saber: imagens, áudio, vídeo, jogos e programas de qualquer tipo;

8.5.6. Acessar *sites* não confiáveis que possam apresentar vulnerabilidades de segurança ou que possam comprometer de alguma forma a segurança e integridade da rede corporativa e da segurança da informação.

8.6. É vedado aos usuários:

8.6.1. Utilizar-se de quaisquer meios que visem contornar os mecanismos de proteção e auditoria de acesso da rede corporativa do Tribunal ou que objetivem descaracterizar o acesso indevido às páginas ou serviços proibidos no artigo anterior;

8.6.2. Instalar em qualquer computador *softwares* que não tenham sido homologados pela SETIC, bem como a edição ou a execução de quaisquer arquivos alheios às atividades laborais;

8.6.3. Copiar programas de computador, licenças de *software* e sistemas implantados nas estações de trabalho, quer seja para uso externo, quer seja para uso em outra estação de trabalho do órgão;

8.6.4. Instalar quaisquer periféricos, componentes ou placas de *hardware* que não tenham sido adquiridos pelo Tribunal, exceto nos casos de comprovada necessidade e com acompanhamento de técnico qualificado da SETIC;

8.6.5. Conectar dispositivos não institucionais, portáteis ou não, na rede corporativa;

8.6.6. Conectar qualquer dispositivo, seja ativo ou passivo, independente de seu propósito, na rede corporativa, exceto aqueles homologados pela SETIC;

8.6.7. Utilizar qualquer tipo de tecnologia *wireless* que venha interferir no correto funcionamento da rede *wireless* do Tribunal, incluindo *access-points*, *bluetooth*, ancoragem *wi-fi*, etc;

8.6.8. Conectar qualquer dispositivo institucional em redes cabeadas ou sem fio não homologadas/institucionais, ou através de modems 3G/4G, exceto nos casos previamente autorizados pela SETIC;

8.6.9. Fazer acesso a sistemas de correio eletrônico que não sejam homologados pela SETIC;

8.6.10. Fornecer relação de endereços eletrônicos dos usuários do Tribunal para terceiros;

8.6.11. Armazenar, nas unidades de rede ou nas soluções baseadas em nuvem, arquivos não relacionados com as atividades institucionais, tais como: músicas, vídeos, fotos etc.

8.7. O acesso aos *sites* e serviços que estejam enquadrados como uso indevido, mas que sejam necessários ao desempenho das atribuições funcionais do usuário será liberado mediante solicitação com justificativa formal direcionada à SETIC.

8.8. A SETIC registrará os endereços das páginas acessadas pelos usuários e, sendo comprovada a utilização indevida do serviço de acesso à *internet*, o referido acesso será bloqueado ou restringido, com comunicação enviada ao superior hierárquico e, a depender dos riscos desta utilização, estes acessos serão apresentados ao Comitê de Segurança da Informação para tomada de providências.

8.9. Os parâmetros de configuração dos computadores serão definidos pela SETIC, que levará em conta os requisitos de segurança, estabilidade, confiabilidade e padronização do ambiente computacional e da rede corporativa e não devem ser alterados pelos usuários a menos que seja orientado a fazê-lo pelos profissionais de suporte da SETIC.

8.10. Os *softwares* utilizados no ambiente computacional somente poderão ser instalados nas estações de trabalho por servidores da SETIC ou técnicos devidamente autorizados pela SETIC.

9. Do correio eletrônico e serviços de mensagens instantâneas

9.1. Aos magistrados e servidores do quadro efetivo em atividade, servidores cedidos ou requisitados de outros órgãos e ocupantes de cargo em comissão lotados no TRT da 14ª Região, será fornecida conta para acesso ao sistema de Correio Eletrônico (*e-mail*) e Comunicador Interno Institucional (*Chat*), que deverão ser utilizados de forma restrita para os objetivos e funções próprias e inerentes às suas atribuições e atividades funcionais.

9.2. A disponibilização de conta de e-mail e comunicador instantâneo a estagiários e colaboradores terceirizados é restrita e somente será realizada se atendidas, cumulativamente, as seguintes condições:

9.2.1. Existência de solicitação formal e fundamentada do chefe da unidade na qual estes colaboradores estiverem lotados;

9.2.2. Disponibilidade de licenças do serviço (contas ociosas) para atribuição imediata;

9.2.3. Deliberação e aprovação de cada solicitação pelo Comitê de Segurança da Informação.

9.3. O e-mail institucional é um instrumento de comunicação do TRT da 14ª Região que deve ser utilizado exclusivamente nas atividades laborais. É vedada a utilização do endereço corporativo na criação de contas particulares em plataformas de redes sociais ou qualquer tipo de conta na internet relacionada a webcommerce, streaming e serviços similares que não estejam ligados diretamente às atividades laborais.

9.4. As ferramentas de Correio Eletrônico e Comunicador Interno (*Google Chat*) são as principais ferramentas de comunicação e devem, de forma obrigatória, ser acessadas diariamente por todos os usuários.

9.5. Em caráter excepcional, o serviço de mensagens instantâneas *WhatsApp Web* poderá ser liberado às unidades que justificarem ser necessário, conveniente e adequado utilizá-lo com o propósito exclusivo de assuntos de interesse institucional do TRT14.

9.5.1. A liberação do acesso ao WhatsApp Web deverá ser solicitada à SETIC por meio de chamado técnico realizado via SAU, indicando qual o nome do usuário que terá acesso ao citado serviço.

9.5.2. Para a concessão de acesso ao WhatsApp Web, o solicitante deverá preencher o termo de consentimento e responsabilidade fornecido pelo suporte ao usuário no momento da solicitação.

9.5.2.1. Caso o WhatsApp Web seja solicitado pelo estagiário(a), o termo de consentimento deverá ser preenchido e assinado pelo gestor da unidade responsável.

9.5.3. A utilização do serviço tratado no item 8.5 é restrita a acessos realizados por contas associadas a números de telefones corporativos do TRT14 (celular ou fixo), pelo aplicativo *WhatsApp Business*.

9.5.4. O uso do serviço *WhatsApp Web* está restrito unicamente a assuntos de interesse institucional do TRT14, não sendo permitido, em hipótese alguma, sua utilização para finalidade diversa.

9.5.5. Dentro da rede corporativa, é vedado o recebimento de qualquer tipo de arquivo através do serviço WhatsApp Web, salvo nos casos em que controles adicionais tenham sido criados e implementados pela divisão de segurança da informação.

9.6. Os usuários devem manter os serviços de chat e e-mail ativos (*online)* sempre que o uso dos computadores estiver sendo realizado, mantendo-os ativos durante toda a jornada de trabalho.

9.7. As contas de correio eletrônico dos usuários serão desativadas e excluídas após 30 dias do desligamento do quadro funcional do Tribunal.

9.7.1. O eventual *backup* das mensagens e arquivos armazenados nas contas deverá ser solicitado à SETIC dentro do prazo supradescrito.

9.7.2. A exclusão da conta implicará na impossibilidade permanente de recuperação das mensagens e arquivos vinculados a ela.

9.7.3. O magistrado ou servidor efetivo desligado do quadro funcional deverá informar à Secretaria de Gestão de Pessoas um endereço de correio eletrônico pessoal, o qual será usado para os casos de comunicação de assuntos do seu interesse.

9.7.4. Para os fins deste artigo, considera-se desligamento do quadro funcional qualquer situação que desvincule o magistrado ou servidor da prestação de suas atividades funcionais ligadas diretamente ao TRT da 14ª Região, tais como: vacância, exoneração, aposentadoria, remoção, cedência, distribuição para outro órgão, falecimento etc.

9.8. O usuário deverá manter a capacidade de armazenamento de sua caixa postal dentro dos limites fornecidos pela SETIC, prezando pela limpeza periódica, eliminando mensagens desnecessárias.

9.9. Caracteriza-se uso inapropriado do serviço de correio eletrônico e serviços de mensagens instantâneas, enviar mensagens contendo:

9.9.1. Texto obsceno, ilegal, antiético, preconceituoso, discriminatório ou que atente flagrantemente a moral ou os bons costumes;

9.9.2. Conteúdo calunioso ou difamatório;

9.9.3. Listas de endereços eletrônicos dos usuários do Correio Eletrônico do Tribunal;

9.9.4. Vírus ou qualquer programa danoso;

9.9.5. Material de natureza político-partidária ou sindical, que promova a eleição de candidatos para cargos públicos eletivos, clubes, associações e sindicatos, bem como material protegido por leis de propriedade intelectual;

9.9.6. Entretenimentos e correntes;

9.9.7. Assuntos ofensivos;

9.9.8. Imagens, áudio ou vídeo que não estejam relacionados ao desempenho das atividades funcionais;

9.9.9. Arquivos executáveis de qualquer tipo;

9.9.10. Mensagens comerciais não solicitadas, também conhecidas como *spam*;

9.9.11. Outros conteúdos notadamente fora do contexto do trabalho desenvolvido.

9.10. A ETIR - Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação da SETIC, deverá ser comunicada sempre que o usuário receber mensagens com os conteúdos descritos acima ou de remetentes desconhecidos e duvidosos que possam oferecer riscos à segurança da rede corporativa.

9.10.1. A comunicação à ETIR deve ser realizada por meio de mensagem de e-mail para o endereço etir@trt14.jus.br.

10. Do serviço de armazenamento de arquivos eletrônicos

10.1. A SETIC oferecerá serviços de armazenamento de arquivos eletrônicos a todos os magistrados e servidores em atividade e, excepcionalmente, a estagiários e outros usuários que, comprovadamente, necessitem do serviço para realização de trabalhos de interesse do TRT14.

10.2. O serviço de armazenamento de arquivos eletrônicos de que trata o artigo anterior será oferecido em duas modalidades:

10.2.1. Serviço de armazenamento de arquivos em rede: consiste em espaço de armazenamento de arquivos eletrônicos totalmente gerido pela SETIC que apresenta as seguintes características técnicas e operacionais:

10.2.1.1. Está hospedado na infraestrutura de datacenter do TRT14;

10.2.1.2. Tem capacidade limitada de acordo com a capacidade de infraestrutura disponível, atos e políticas da SETIC e com a natureza das atividades desenvolvidas pelos usuários;

10.2.1.3. Possui mecanismos de prevenção contra uso abusivo, tais como rejeição de arquivos de determinados tipos, rejeição de arquivos únicos com tamanho exagerado e outros controles, como descritos em políticas de armazenamento e segurança da SETIC;

10.2.1.4. Está coberto pela Política de *Backup* e Recuperação de arquivos da SETIC TRT14, com exceção das unidades de armazenamento de transferência temporária (por exemplo, unidade T, ou transfer).

10.2.2. Serviço de armazenamento em nuvem: consiste em espaço de armazenamento de arquivos eletrônicos parcialmente gerido pela SETIC que apresenta as seguintes características técnicas e operacionais:

10.2.2.1. Está hospedado em infraestrutura terceirizada (contratada) de computação em nuvem;

10.2.2.2. Tem capacidade limitada de acordo com os atos e políticas da SETIC e as limitações inerentes às contratações que regem os respectivos serviços;

10.2.2.3. Pode não fornecer meios de recuperação de arquivos totalmente apagados;

10.2.2.4. Pode possuir funcionalidades de compartilhamento de arquivos com outros usuários, inclusive externos ao TRT14, sendo responsabilidade de cada usuário os efeitos decorrentes do uso deste recurso;

10.2.2.5. Os arquivos armazenados nos drives compartilhados possuem como proprietário o Tribunal. Desta forma, após o desligamento do usuário, o encerramento de sua conta não ocasiona a perda das informações ali armazenadas;

10.2.2.6. Desde que expresso pelo proprietário, caso houver necessidade de migração dos arquivos armazenados no “Meu Drive”, este deverá solicitar a mudança de

proprietário dos arquivos de relevância para a instituição ou transferi-los para um drive compartilhado correspondente à sua unidade.

10.3. Visando proteger as informações institucionais, os usuários devem manter, sempre que possível, cópia dos arquivos de trabalho locais (hospedados apenas na estação de trabalho) em um dos serviços de armazenamento de arquivos eletrônicos especificados nos itens 9.2.1 e 9.2.2.

10.3.1. Em relação à geração e armazenamento de dados, os usuários devem observar a legislação vigente relacionada ao tratamento de dados pessoais e sensíveis, sendo proibido armazenar dados em desacordo com estas políticas nos serviços de armazenamento de rede definidos neste item e, principalmente, em unidades de armazenamento locais, como por exemplo, discos rígidos de estações de trabalho ou unidades de armazenamento externas.

10.3.2. Arquivos com dados pessoais ou sensíveis só podem ser mantidos armazenados localmente (nas estações de trabalho) pelo tempo necessário à realização do trabalho que motivou sua manipulação.

11. Do acesso aos Recursos de TIC

11.1. O acesso ao Centro de Dados do Tribunal e demais equipamentos de TIC - servidores de rede, computadores, *notebooks*, *scanners*, impressoras, multifuncionais, *racks*, *switches*, roteadores e outros - está restrito aos servidores da SETIC ou aos técnicos terceirizados devidamente autorizados pela SETIC.

11.2. Visando manter o adequado monitoramento dos serviços, o correto funcionamento da infraestrutura de rede, a longevidade dos equipamentos e atender aos requisitos de garantia, todos os equipamentos de rede (*switches*, roteadores, modens etc) devem permanecer energizados por *no-break*, ligados e conectados, exceto em casos previamente autorizados pela SETIC.

11.3. Eventual pedido de movimentação de equipamentos de TIC deverá ser feito pelos Gestores das unidades judiciárias ou administrativas, informando os motivos da solicitação à SETIC, a quem compete analisar a viabilidade técnica do pedido.

11.4. As movimentações internas e externas de equipamentos de TIC deverão ser registradas no Sistema de Movimentação de Bens, conforme regulamentação própria, sendo executadas pela SETIC ou pelo setor patrimonial do Tribunal.

11.4.1. Excepcionalmente, por necessidade de serviço, os magistrados e os diretores das unidades judiciárias e administrativas poderão autorizar a remessa à SETIC ou a retirada de estações de trabalho, servidores de rede, impressoras e outros equipamentos por funcionários devidamente identificados, registrando-se a ocorrência.

11.4.2. No caso de equipamentos retirados para manutenção, por empresa contratada para tal finalidade, deverá ser utilizado documento de autorização fornecido pela Secretaria de Tecnologia da Informação.

11.5. O acesso a dispositivos de armazenamento externos como *pen drives*, *HDs externos* e similares é vedado e possui bloqueio automático aplicado em todos os computadores corporativos. A eventual liberação de acesso desse tipo de dispositivo poderá ser realizada após a necessidade ter sido devidamente formalizada com justificativa relacionada diretamente às atividades laborais e, mediante avaliação da área de Segurança da Informação da SETIC, que sempre levará em conta os riscos associados.

12. Da Gestão e Controle de Ativos de Informação

12.1. O processo de Gestão e Controle de Ativos de Informação deverá ser instituído com o objetivo principal de implementar um conjunto coordenado de atividades voltadas para assegurar a preservação e o uso adequado dos ativos de informação institucionais, por meio do acompanhamento do seu ciclo de vida, desde a sua compra até o seu descarte.

12.2. O processo de que trata o caput deverá contemplar, no mínimo, as seguintes etapas: cadastro, atualização e exclusão de ativos.

12.3. Caberá aos gestores dos ativos de informação a execução do processo de Gestão e Controle de Ativos de Informação, sob a supervisão da Divisão de Segurança da Informação da Secretaria de Tecnologia da Informação e Comunicação.

12.4. O tratamento de ativos não autorizados será realizado através da implementação do protocolo 802.1x, ou, na sua ausência, pelo bloqueio ou liberação de seu acesso através do uso dos recursos disponíveis, nos termos deste ato.

13. Das disposições finais

13.1. Cada usuário é responsável pela Segurança da Informação do Órgão e deve conhecer, entender e cumprir as diretrizes, normas, procedimentos e instruções integrantes da Política de Segurança da Informação, zelando pela correta aplicação das medidas de proteção.

13.2. O usuário que apagar, destruir, modificar ou, de qualquer forma, inutilizar, total ou parcialmente, arquivo ou programa de computador, fizer uso indevido ou não autorizado dos equipamentos de TIC, bem como agir em desacordo com os termos deste ato fica sujeito à aplicação das penalidades administrativas, civis e penais cabíveis.

13.2.1. O disposto no item 11.2 aplica-se aos prestadores de serviços, aos estagiários, aos servidores e empregados de órgãos conveniados, no que couber.

13.2.2. Os diretores das unidades judiciárias e administrativas, verificando a existência de indícios de materialidade de qualquer fato descrito no item 11.2, comunicarão a ocorrência, de

imediato, ao superior hierárquico para adoção das providências cabíveis.

13.3. A SETIC deverá gerir a infraestrutura necessária para prover com segurança os serviços disponíveis na rede corporativa, assim como o acesso às redes externas, desenvolvendo as ações necessárias para o cumprimento deste ato.

13.4. Os casos omissos e as dúvidas surgidas na aplicação deste ato serão dirimidos pelo Comitê de Segurança da Informação, pelo Comitê de Gestão de TIC (CGesTIC) e pelo Comitê de Governança de TIC (CGTIC).

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO
Gabinete da Presidência

PORTARIA GP N.º 0581, DE 29 DE MAIO DE 2024.

ANEXO IV

NSI04 – Gestão de Incidentes de Segurança da Informação

1. Objetivos

1.1. Estabelecer as diretrizes e definir o processo de Gestão de Incidentes de Segurança da Informação relacionada ao ambiente tecnológico no âmbito deste Tribunal.

2. Motivações

2.1. Alinhamento às normas, regulamentações e melhores práticas, relacionadas à matéria

2.2. Necessidade de tratar os incidentes de segurança da informação com resposta rápida e eficiente.

2.3. Correto direcionamento e dimensionamento de recursos tecnológicos e humanos para prover uma Gestão de Incidentes de Segurança da Informação com menor custo e maior qualidade.

2.4. Formalização de um processo sistemático para gerenciamento dos incidentes de segurança da informação, provendo insumos para minimizar e/ou evitar eventos futuros.

3. Referências normativas

3.1. Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14.08.2009, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

3.2. Norma Complementar nº 08/IN01/DSIC/GSIPR, de 14.08.2010, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina o gerenciamento de

Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais – ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

3.3. Norma Técnica 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.

3.4. Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação.

3.5. Norma Complementar nº 21/IN01/DSIC/GSIPR, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.

3.6. Norma Técnica ISO/IEC 27000:2018, que especifica conceitos e definições relacionados às normas de segurança da informação.

4. Conceitos e definições

4.1. **Artefato malicioso:** é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores.

4.2. **Ativos de Informação:** os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

4.3. **Usuários:** magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários, e outras pessoas que se encontrem a serviço da Justiça do Trabalho, utilizando em caráter temporário os recursos tecnológicos do TRT.

4.4. **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR:** Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

4.5. **Evento de segurança da informação:** ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política

de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

4.6. **Incidente de segurança da informação:** é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados,que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

4.7. **Medida de contenção:** controle e/ou ação tomada para evitar que danos causados por um determinado incidente continuem aumentando com o passar do tempo. Além disso, tais medidas visam o restabelecimento do sistema/serviço afetado, mesmo eu não seja em sua capacidade total.

4.8. **Medida de solução:** controle e/ou ação tomada para sanar vulnerabilidades e problemas que sejam a causa-raiz de um ou mais incidentes de segurança da informação.

4.9. **Tratamento de Incidentes de Segurança em Redes Computacionais:** é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

4.10. **Vulnerabilidade:** fragilidade de um ativo ou controle que pode ser explorado por uma ameaça.

4.11. **CTIR GOV:** Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI;

5. Escopo

5.1. A Gestão de Incidentes de Segurança da Informação, definida nesta norma, tem seu escopo limitado às situações relacionadas ao ambiente, ativos, projetos e processos de TIC.

6. Interface com demais processos

6.1. A seguir estão descritas as principais interfaces e/ou subprocessos do processo de gerenciamento de incidentes de segurança da informação com os demais processos de TIC:

- **Gerenciamento de eventos de TIC**: desenvolvimento e implementação de atividades adequadas à descoberta oportuna de eventos ou à detecção de incidentes de segurança cibernética. Estão contempladas ações de monitoramento contínuo de segurança, processos de detecção de anomalias e eventos.
- **Gerenciamento de Configuração e Ativos de Serviço:** interação para assegurar que os ativos requeridos para a entrega de um serviço sejam adequadamente controlados, com informações seguras.
- **Gerenciamento de incidentes de TIC**: o processo pode ser iniciado através de um incidente que já estava em tratamento no processo de gerenciamento de incidentes.
- **Subprocesso Gerenciar Crise Cibernética**: Subprocesso executado para iniciar as ações necessárias para gerenciar uma Crise Cibernética quando identificada.

7. Diretrizes

7.1. A Gestão de Incidentes de Segurança da Informação tem como principal objetivo assegurar que incidentes de segurança da informação sejam identificados, registrados e avaliados em tempo hábil, com a tomada de medidas de contenção e/ou solução adequada.

7.2. Estão abrangidos por esta norma os eventos, confirmados ou suspeitos, relacionados à segurança de sistemas ou redes computacionais que comprometam o ambiente tecnológico do TRT, seus ativos, informações e processos de negócio, bem como aqueles que contrariem a Política de Segurança da Informação deste Tribunal, e dos quais decorram interrupção, parcial ou total, de serviço essencial ao desempenho das atividades, vulnerabilidades de segurança, divulgação, alteração ou destruição de informações e/ou prática de ato definido como crime ou infração administrativa.

7.3. O Tribunal providenciará dispositivos de monitoramento, ferramentas de segurança e detecção de intrusão, a fim de subsidiar a Gestão de Incidentes de Segurança da Informação.

8. O processo de Gestão de Incidentes de Segurança da Informação

8.1. Estabelecer as diretrizes para o funcionamento da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR) do Tribunal Regional do Trabalho da 14ª Região.

8.2. O processo de Gestão de Incidentes de Segurança da Informação é composto pelas seguintes etapas:

8.2.1. **Detecção:** compreende o recebimento, registro e autorizações necessárias para o encaminhamento da investigação;

8.2.2. **Investigação e triagem:** compreende a investigação e tratamento do incidente, coleta de dados, comunicação às áreas

afetadas, proposição de ações de contenção, quando necessárias;

8.2.3. **Análise e Resposta:** compreende a execução das ações propostas pela etapa investigação e triagem, através de ações de contenção e resposta, bem como a geração de evidências;

8.2.4. **Encerramento:** compreende a análise do incidente, com verificação da necessidade de outras ações, providências ou comunicações, e após seu cumprimento, o encerramento do incidente;

8.2.5. **Avaliação de incidentes:** compreende a avaliação do histórico de incidentes, com consolidação das informações e indicadores e verificação das oportunidades de melhoria e lições aprendidas.

8.3. Os incidentes, notificados ou detectados, devem ser objeto de registro, com a finalidade de assegurar a manutenção do histórico e auxiliar na geração de indicadores.

8.4. A notificação de incidente poderá ser feita por qualquer usuário, sem necessidade de prévia autorização do gestor, através do sistema de chamado ou diretamente a Divisão de Segurança da Informação, pelo chat, telefone ou pelo e-mail etir@trt14.jus.br, que a reportará a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação.

8.5. Os usuários devem notificar, o mais breve possível, sobre os incidentes de segurança da informação e vulnerabilidades de que tenham conhecimento (observada ou suspeita).

8.6. Vulnerabilidades ou fragilidades suspeitas não deverão ser objeto de teste ou prova pelos usuários, sob o risco de violar a política de segurança da informação e/ou provocar danos aos serviços ou recursos tecnológicos.

8.7. As equipes da Secretaria de Tecnologia da Informação responsáveis pelo monitoramento dos ativos, serviços e sistemas devem notificar os incidentes a eles relacionados à Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação, para o devido registro e encaminhamento.

8.8. O Tribunal poderá receber notificações externas (CTIR.BR ou outras empresas) sobre incidentes (ocorridos ou suspeitos) por meio de sistemas gerenciadores de demandas, e-mail, telefone, etc, que deverão ser remetidas à Divisão de Segurança da Informação, para o devido encaminhamento.

8.9. O tratamento da informação deve ser realizado de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação, com retorno das operações à

normalidade no menor prazo possível, bem como evitar futuras ocorrências, com a proposição de ações de solução, quando existentes.

8.10. A Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação deve conduzir, apoiada pelas outras áreas da SETIC, investigação do incidente e artefatos maliciosos, propondo e implementando as ações de contenção, comunicando as áreas afetadas e coletando os dados necessários.

8.11. A coleta de evidência dos incidentes de segurança da Informação deve ser realizada pela Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação ou por pessoal competente e por ela autorizado.

8.12. 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.

8.13. Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, o Comitê de Segurança da Informação e a Administração do TRT deverão ser comunicados para avaliação das providências cabíveis.

8.14. O encerramento do incidente de segurança da informação será realizado pela Divisão de Segurança da Informação, com comunicação a todas as áreas interessadas e ao Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR.BR) na forma e nos casos definidos pelo referido órgão.

8.15. A avaliação do processo de gestão de incidentes de segurança da informação ocorrerá através do histórico de incidentes, com verificação das oportunidades de melhoria.

8.16. O processo será revisto anualmente ou em menor prazo, quando necessário. Eventuais alterações propostas nos documentos acima indicados serão objeto de imediata divulgação na forma do item anterior, após aprovação pela Presidência deste TRT.

9. Incidentes ocorridos nos serviços em nuvem

9.1. O Gestor de Segurança da Informação deverá comunicar incidentes cibernéticos informados pelo provedor de serviço de nuvem aos órgãos competentes para os seus tratamentos, conforme a relevância dos

incidentes previamente estabelecida

9.2. O provedor de serviço de nuvem deverá:

I. registrar todos os acessos, incidentes e eventos cibernéticos, incluídas informações sobre sessões e transações, armazenando pelo período mínimo de um ano;
II. armazenar os registros de todos os acessos, incidentes e eventos cibernéticos, incluindo informação sobre sessões e transações, por cinco anos, no ambiente do provedor de serviço de nuvem ou em ambiente próprio controlado, à critério do órgão ou da entidade contratante;
III. manter em ambiente próprio controlado, pelo período de cinco anos, os registros de todos os acessos, incidentes e eventos cibernéticos, incluindo informação sobre sessões e transações recebidos do provedor de serviço de nuvem; e
IV. capacitar a equipe de segurança para acessar e utilizar os registros gerados pelo provedor de serviço de nuvem.

10. Gerenciamento da Crise Cibernética

10.1. O Gerenciamento da Crise Cibernética prevê as ações responsivas a serem colocadas em prática quando ficar evidente que um incidente de segurança cibernética não será mitigado rapidamente e poderá durar dias, semanas ou meses

11. Identificação de Crise Cibernética

11.1. A ETIR comunicará ao Subcomitê de Crises Cibernéticas, tempestivamente, a ocorrência de qualquer incidente que constituir ou der início a uma crise cibernética.

11.2. O gerenciamento de incidentes se refere às atividades que devem ser executadas na ocorrência de evento adverso de segurança da informação, para avaliar o problema e determinar a resposta inicial.

11.3. O gerenciamento de crise se inicia quando:

I. Caracterizado grave dano material ou de imagem;
II. For evidente que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período, podendo se estender por dias, semanas ou meses;
III. O incidente impactar a atividade finalística ou o serviço crítico mantido pela organização; ou
IV. O incidente atrair grande atenção da mídia e da população em geral.

12. Execução (Durante a Crise)

12.1. O Subcomitê de Crises Cibernéticas deve coordenar ações para garantir que a comunicação entre as áreas envolvidas em crise seja

tratada como fator crítico para uma organização responder a uma crise cibernética de longa duração ou de grande impacto.

12.2. Assim que a ETIR identificar que um incidente constitui crise cibernética, deverá ser reunido imediatamente o Subcomitê de Crises Cibernéticas.

12.3. As etapas e procedimentos de resposta são diferentes de acordo com o tipo de crise e são necessárias reuniões regulares para avaliar o progresso até que seja possível retornar à condição de normalidade.

12.4. Os incidentes graves que ocasionam a deflagração de uma crise cibernética deverão ser comunicados ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), órgão superior vinculado ao Conselho Nacional de Justiça, de acordo com a Portaria CNJ 162/2021, Anexo II, item 5.9.

12.5. Deverá ser comunicado à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Sendo esta comunicação feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I. a descrição da natureza dos dados pessoais afetados;
II. as informações sobre os titulares envolvidos;
III. a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
IV. os riscos relacionados ao incidente;
V. os motivos da demora, no caso de a comunicação não ter sido imediata; e
VI. as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

13. Fase de Melhoria Contínua (Lições Aprendidas no Pós-Crise)

13.1. Quando as operações retornarem à normalidade, o Subcomitê de Crises Cibernéticas deverá realizar a análise criteriosa das ações tomadas, observando as que foram bem-sucedidas e as que ocorreram de forma inadequada.

13.2. Para a identificação das lições aprendidas e a elaboração de relatório final, deve ser objeto de avaliação:

- a identificação e análise da causa do incidente;
- a linha do tempo das ações realizadas;
- a escala do impacto nos dados, sistemas e operações de negócios importantes durante a crise;
- os mecanismos e processos de detecção e proteção existentes e as necessidades de melhoria identificadas;
- o escalonamento da crise;
- a investigação e preservação de evidências;

- a efetividade das ações de contenção;
- a coordenação da crise, liderança das equipes e gerenciamento de informações; e
- a tomada de decisão e as estratégias de recuperação.

13.3. As lições aprendidas devem ser utilizadas para a elaboração ou revisão dos procedimentos específicos de resposta e a melhoria do processo de prevenção de crises cibernéticas.

13.4. 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.

13.5. Ao final de uma situação de crise, será elaborado relatório final de tratamento do incidente cibernético, considerando:

- Informações sobre a gestão do incidente, como as equipes envolvidas, as decisões tomadas durante o tratamento do incidente cibernético, as ações de contenção e recuperação empregadas, etc;
- identificação e análise da causa-raiz do incidente cibernético;
- a linha do tempo das ações realizadas;
- impacto identificado nos dados e ambiente computacional;
- informações a respeito da coleta e preservação das evidências identificadas;
- ações objetivas sugeridas para diminuir a probabilidade da ocorrência de incidentes similares ou diminuir o impacto caso eles ocorram;
- as oportunidades de melhoria de processo, de tecnologia ou de gestão identificadas.

14. Coleta e Preservação de Evidências Digitais

14.1. A ETIR deverá elaborar e executar procedimentos para a coleta e preservação de evidências digitais, tais como:

- as mídias de armazenamento envolvidas no incidente cibernético ou suas imagens forenses;
- os dados voláteis armazenados nos equipamentos, como memória RAM;
- os logs locais e remotos relacionados.

14.2. As ações de restabelecimento do serviço não devem comprometer a coleta e preservação da integridade das evidências.

14.3. Quando não for possível a preservação das mídias de armazenamento dos dispositivos afetados em virtude da necessidade do restabelecimento do serviço afetado, a pessoa responsável pela ETIR deverá supervisionar a coleta de todos os dados necessários para a investigação do incidente cibernético, tais como logs, arquivos e configurações do sistema operacional, dentre outros, respeitando-se a

estrutura e os metadados dos arquivos originais, como data e hora de criação e as permissões vigentes.

14.4. Quando não for possível a preservação das mídias de armazenamento dos dispositivos afetados, a pessoa responsável, da ETIR, deverá fazer constar em relatório a impossibilidade de preservação das mídias afetadas e listará todos os procedimentos adotados.

14.5. Para a preservação da integridade das informações, será gerado arquivo com a lista de todos os arquivos coletados e seus respectivos resumos criptográficos (hashes). Deverá, também, ser gerado resumo criptográfico do arquivo que contém esta lista.

14.6. O material coletado será lacrado e custodiado pela pessoa responsável pela ETIR, ou por servidor(a) indicado(a) por ela, e ficará a disposição da Administração ou das autoridades acionadas para a continuidade das investigações.

14.7. Quando for identificado incidente penalmente relevante, a ETIR comunicará imediatamente à Administração para o início das tratativas com as autoridades competentes.

15. Atualização da norma

15.1. As diretrizes previstas na presente norma serão atualizadas sempre que alterados os procedimentos da Gestão de Incidentes de Segurança da Informação, observada a periodicidade prevista para a revisão da Política de Segurança da Informação.

TABELA DO PLANO DE GESTÃO DE INCIDENTES CIBERNÉTICOS			
Incidente Cibernético	**Descrição**	**Severidade**	**Procedimento**
Campanha de phishing	O órgão é alvo de uma campanha de phishing	Média	**Link**
Degradação de serviços	Degradação ou interrupção de serviços ou sistemas por ataque de negação de serviço (DoS)	Alta	**Link**
Comprometimento de credenciais	Comprometimento de credenciais com acesso a informações sensíveis	Alta	**Link**
Ataque de ransomware	Importantes informações organizacionais inacessíveis por encriptação (ransomware)	Crítica	**Link**
Vazamento de informações internas	Informações críticas encontradas fora da organização	Crítica	**Link**
Ataque de malware	Infecção de sistemas por malware	Alta	**Link**
Roubo de identidade	Uso indevido de informações pessoais para obter benefícios financeiros	Alta	**Link**
Ataque de engenharia social	Manipulação psicológica para obter informações confidenciais	Alta	**Link**
Ataque de injeção de código	Inserção de código malicioso para explorar	Alta	**Link**

	vulnerabilidades		
Ataque de brute force	Tentativas repetitivas de adivinhar senhas por meio de força bruta	Média	**Link**
Exploração de vulnerabilidade conhecida	Aproveitamento de uma vulnerabilidade previamente identificada para obter acesso não autorizado	Alta	**Link**

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO
Gabinete da Presidência

PORTARIA GP N.º 0581, DE 29 DE MAIO DE 2024.

ANEXO V

NSI05 – Gestão de Riscos de Tecnologia da Informação e Comunicações

1. Objetivos

1.1. Estabelecer as diretrizes da gestão de riscos de TIC relacionada ao ambiente tecnológico no âmbito deste Tribunal, aos projetos e processos de Tecnologia da Informação e Comunicações (TIC), e definir o processo de Gerenciamento de Riscos de Tecnologia da Informação e Comunicações do TRT da 14ª Região (GRTIC-TRT14).

2. Aplicabilidade

2.1. Este documento aplica-se a todas as unidades pertencentes à Secretaria de Tecnologia da Informação e Comunicação responsáveis por gerenciar, manipular e operar informações, projetos, processos, produtos e serviços relacionados à área de TIC no âmbito do TRT da 14ª Região

3. Motivações

3.1. Necessidade de um processo sistemático para gerenciar riscos referentes à Tecnologia da Informação e Comunicações (TIC), projetos e processos de TIC, provendo insumos para aumentar a proteção contra eventos indesejados.

3.2. Correto direcionamento de esforços e investimentos financeiros, tecnológicos e humanos.

3.3. Conformidade com normatizações e regulamentações relacionadas ao assunto.

4. Referências normativas

4.1. Norma Técnica ABNT NBR ISO/IEC 27005:2019, que fornece diretrizes para o processo de gestão de riscos de Segurança da Informação.

4.2. Norma Técnica ABNT NBR ISO 31000:2018, que fornece princípios e diretrizes genéricas para a gestão de riscos.

4.3. Norma ABNT NBR ISO/IEC 27002:2013, que trata do Código de Prática para a Gestão da Segurança da Informação.

4.4. Norma Técnica 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 do contexto da organização.

5. Conceitos e definições

5.1. **Ameaça** - causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização;

5.2. **Análise de riscos** - processo para compreender a natureza do risco e determinar seu grau de ameaça;

5.3. **Avaliação de riscos** - processo de comparação dos resultados da análise de risco com critérios de risco para determinar se o risco e/ou sua magnitude são aceitáveis ou toleráveis;

5.4. **Ativos de Informação** - os meios de armazenamento transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

5.5. **Comunicação do risco** - conjunto de processos contínuos e iterativos que uma organização realiza para fornecer, compartilhar ou obter informações e para dialogar com as partes interessadas sobre o gerenciamento de riscos;

5.6. **Compartilhamento do risco –** ação de transferir o risco para um terceiro.

5.7. **Estimativa de riscos** - processo utilizado para atribuir valores à probabilidade e às consequências de um risco;

5.8. **Evitar risco** - forma de tratamento de risco pela qual se decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco;

5.9. **Gestão de Riscos de Tecnologia da Informação e Comunicações (GRTIC–TRT14)** - conjunto de atividades que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

5.10. **Gestão de Riscos em Projetos de TIC** - conjunto de atividades que envolve a identificação, a análise, o planejamento de respostas, o monitoramento e o controle de riscos de um projeto.

5.11. **Gestão de Riscos em Processos de TIC** - conjunto de atividades, estabelecidas de acordo com as peculiaridades ou normatividades que regem cada processo, que visam a identificar e minimizar ou eliminar os riscos.

5.12. **Grau do risco -** medida da ameaça potencial que um determinado risco possui. Seu valor é obtido pelo produto entre a probabilidade e o impacto intrínseco a cada risco.

5.13. **Identificação de riscos** - processo para localizar, listar e caracterizar elementos de risco.

5.14. **Impacto -** efeitos no ambiente se um evento de risco ocorrer.

5.15. **Modificação do risco –** ação de implementar salvaguardas/controles aos riscos de modo a reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco;

5.16. **Prioridade -** preferência conferida a um elemento ou decisão em detrimento de outro em função de uma regra de priorização.

5.17. **Probabilidade -** a possibilidade de uma ameaça se concretizar.

5.18. **Reter risco** - forma de tratamento de risco pela qual se decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado;

5.19. **Riscos de Tecnologia da Informação e Comunicações** - potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

5.20. **Tratamento dos riscos** - processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;

5.21. **Vulnerabilidade** - fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças.

6. Escopo

6.1. A Gestão de Riscos, definida por esta Norma, tem seu escopo limitado às medidas protetivas dos ativos de informação bem como dos projetos e processos relacionados à área de TIC que suportam os principais processos de negócio do TRT da 14ª Região.

7. Diretrizes

7.1. A Gestão de Riscos leva em consideração as definições do Planejamento Estratégico Institucional, do Planejamento Estratégico de TIC vigente, do Plano Diretor de TIC do TRT da 14ª Região e das definições deliberadas no Comitê de Segurança da Informação, e está alinhada à Política de Segurança da Informação deste Tribunal.

7.2. A Gestão de Riscos é abordada de forma sistemática, com o objetivo de manter os riscos em níveis aceitáveis para cada projeto, processo e/ou serviço analisado.

7.3. Os riscos são analisados e avaliados em função de sua relevância para os principais processos de negócio deste Tribunal e são tratados de forma a assegurar respostas tempestivas e efetivas.

8. Gestão de riscos em projetos de TIC

8.1. As atividades inerentes ao gerenciamento de riscos em projetos relacionados à TIC devem observar o disposto na metodologia de gerenciamento de projetos adotada pela Secretaria de Tecnologia da Informação de Comunicação.

9. Gestão de riscos em processos de TIC

9.1. A gestão e comunicação de riscos em processos de TIC são definidas na especificação de cada processo e visam à identificação e ao

controle dos eventos que possam comprometer seus objetivos, contribuindo para sua melhoria.

9.2. As atividades inerentes à gestão de riscos nos processos de TIC devem observar as diretrizes desta norma e outras específicas relacionadas ao processo.

9.3. A gestão de riscos em processos de TIC deve ser realizada pelos gestores dos respectivos processos quando de sua confecção e continuamente, durante seu ciclo de vida.

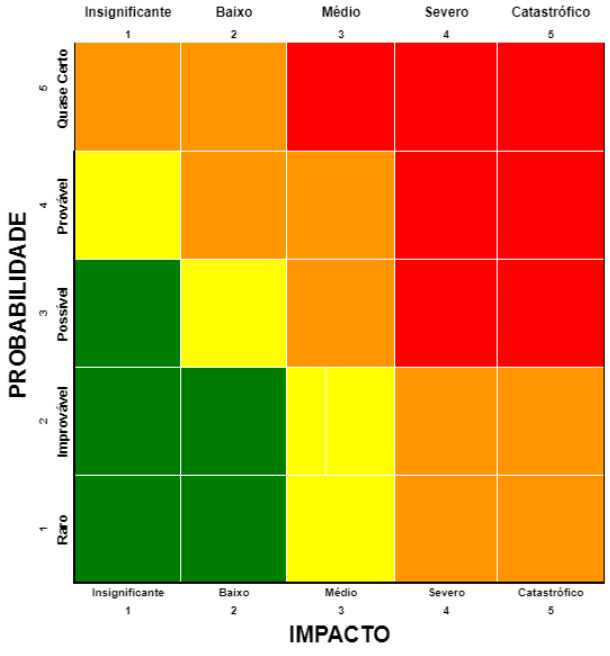
10. Processo de gestão de riscos em Tecnologia da Informação e Comunicações

10.1. O processo de GRTIC-TRT14 é contínuo, fornecendo subsídios e integrando-se à implantação e operação do Sistema de Gestão de Segurança da Informação.

10.2. O processo de GRTIC-TRT14 está baseado nas definições constantes na norma técnica ABNT NBR ISO/IEC 27005:2019.

10.3. O desenho do processo de Gestão de Riscos de Segurança da Informação, a descrição das atividades, respectivos papéis e responsabilidades dos envolvidos no processo, bem como demais documentos relacionados, serão publicados após aprovação pela Presidência.

10.4. Os critérios para avaliação dos riscos levam em consideração duas variáveis: a **probabilidade** de ocorrência e o seu **impacto** potencial. A partir destas duas variáveis são obtidos: a) **o grau dos riscos**, valor que expressa numericamente a força da ameaça (e que resulta do produto entre a probabilidade e o impacto); e b) a **prioridade de tratamento**, que sugere critérios de presteza no tratamento dos riscos. A avaliação do nível de prioridade de tratamento é definida pela interseção entre a probabilidade e impacto do risco na matriz de prioridade abaixo. Do nível resultante (cor), é sugerida uma postura de tratamento.



Nível	Postura de Tratamento Sugerida
I	Riscos pouco significantes. Não são exigidas ações imediatas
B	Riscos não graves. Sugere-se apenas monitoramento regular
M	Riscos de média prioridade. Requerem a definição e execução de ações corretivas para reduzir sua ameaça potencial
A	Riscos prioritários. Exigem a definição e implantação imediata de ações corretivas

10.5. O tratamento dos riscos será definido de acordo com as necessidades levantadas pelas partes interessadas, regulamentações e legislações vigentes, avaliação técnica e análise custo/benefício.

10.6. O processo será revisto anualmente ou em menor prazo, quando necessário. Eventuais alterações propostas nos documentos acima indicados serão, após aprovação pela Presidência deste TRT, objeto de imediata divulgação na forma do item anterior.

11. Atualização da Norma

11.1. As diretrizes previstas na presente norma serão atualizadas sempre que alterados os procedimentos de Gestão de Riscos de TIC, observada a periodicidade prevista para a Política de Segurança da Informação

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO
Gabinete da Presidência

PORTARIA GP N.º 0581, DE 29 DE MAIO DE 2024.

ANEXO VI

NSI06 - Plano de Continuidade dos Serviços Essenciais de TIC

1. CONCEITOS E DEFINIÇÕES

Para os efeitos desta norma, aplicam-se os seguintes conceitos e definições:

Análise de Impacto nos Negócios (AIN): estimativa dos impactos resultantes da interrupção de atividades e de cenários de desastres que possam afetar a prestação jurisdicional do Tribunal, bem como técnicas para quantificar e qualificar esses impactos. Define também a criticidade dos processos de negócio, prioridades, interdependências e os requisitos de segurança da informação e comunicações para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos.

Atividades Críticas: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade, de forma que permitam atingir os objetivos mais importantes e sensíveis ao tempo.

Continuidade de Negócios: capacidade de um órgão ou entidade de, quando ocorrer algum incidente de interrupção, manter suas operações em um nível aceitável, previamente definido, minimizando os impactos e recuperando perdas de ativos da informação das atividades críticas.

Desastre: incidente que tenha causado algum dano grave, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo superior ao aceito pela organização.

Estratégia de Continuidade de Negócios: abordagem de um órgão ou entidade que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou outro incidente maior;

Gestão de Continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado.

Incidente: evento que tenha causado algum dano, colocado em risco, algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

MTPD - Maximum Tolerable Period of Disruption (Período Máximo de Interrupção Tolerável): tempo necessário para que os impactos adversos se tornem inaceitáveis,

que pode surgir como resultado de não fornecer um produto/serviço ou realizar uma atividade.

OMCN - Objetivo Mínimo de Continuidade de Negócios: níveis mínimos aceitáveis de serviços para a organização alcançar seus objetivos de negócios durante uma interrupção.

Plano de Continuidade: conjunto de procedimentos documentados que orientam a organização, após a interrupção, em como responder, recuperar, retomar e restaurar para um nível predefinido de operação, composto por Plano de Continuidade Operacional e Plano de Recuperação de Desastres.

Plano de Continuidade Operacional (PCO): documento que descreve procedimentos operacionais e técnicos a serem realizados frente a determinados cenários de falha, para manutenção dos serviços, ainda que em um nível mínimo de eficiência operacional.

Plano de Recuperação de Desastres (PRD): documento que descreve procedimentos técnicos, focado em ativos e serviços tecnológicos, a serem realizados frente a determinados cenários de falhas dos principais serviços de TIC, visando o retorno à normalidade.

Resiliência: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre.

RPO (Recovery Point Objective): ponto em que a informação usada por uma atividade deve ser restaurada para permitir a operação da atividade na retomada.

RTO (Recovery Time Objective): Tempo máximo para retorno operacional de um serviço ou processo de negócio após a ocorrência de um desastre.

2. DOCUMENTOS DE REFERÊNCIA

Os documentos mais relevantes utilizados como referência para elaboração deste plano estão listados a seguir:

- Res CNJ N. 370/2021 - ENTIC-JUD;
- Res CNJ N. 396/2021 - ENSEC-PJ;
- Portaria GP N. 470/2021, dispõe sobre as soluções de TIC;
- ABNT NBR ISO/IEC 27002:2013;
- ABNT NBR ISO 22313:2015;
- ABNT NBR ISO 22301:2013;
- PCSE-TIC do TRT da 23ª Região.

3. OBJETIVO

Estabelecer as diretrizes e definir o Plano de Continuidade de Serviços Essenciais de Tecnologia da Informação e Comunicações aplicável ao ambiente tecnológico deste Tribunal.

4. ESCOPO

As Soluções de TIC estratégicas são aquelas diretamente fundamentais à prestação jurisdicional do TRT da 14ª Região e demandam, por tal importância, diretrizes especiais que assegurem sua adequada operação e manutenção. As soluções de TIC classificadas como estratégicas, de acordo com a Portaria GP N. 470/2021, são:

I. PJe;
II. PJe-Calc;
III. SISCONDJ;
IV. SIF;

V. Consulta Processual;
VI. AUD;
VII. NAAV;
VIII. GPREC;
IX. JT-E;
X. MNI;
XI. E-REC;
XII. PROAD;
XIII. SIGEP;
XIV. Sistema de Atendimento ao Usuário - SAU;
XV. PORTAL DE INTERNET;
XVI. RDP/VPN;

Considerando a complexidade de elaboração do Plano de Continuidade de Serviços Essenciais de TIC, o escopo atual contemplará os serviços de TIC que ocasionam um maior impacto nas atividades judicantes, conforme a lista abaixo:

I. PJe;
II. PROAD;
III. SIGEP;
IV. SOLUÇÃO DE COMUNICAÇÃO - “GOOGLE WORKSPACE”
V. PORTAL DE INTERNET;
VI. RDP/VPN;

As soluções de TIC estratégicas não contempladas por esta versão inicial do plano, serão adicionadas de acordo com o cronograma de revisões e seu grau de maior relevância.

5. PRINCIPAIS RISCOS E AMEAÇAS

Os principais riscos e ameaças que afetam os serviços essenciais de TIC devem ser identificados e gerenciados, de forma a mitigar o impacto da sua ocorrência na continuidade dos mesmos.

A relação de eventos de desastre evidenciados abaixo, não pretende esgotar todas as possibilidades de acontecimentos danosos, porém contempla de forma macro um mapeamento inicial que deve ser aperfeiçoado ao longo do tempo, de acordo com as revisões previstas neste plano.

A tabela a seguir, descreve os principais riscos e ameaças identificados:

#	EVENTO	CAUSAS POSSÍVEIS
1	**Ataque Cibernético**	• Ataque virtual que comprometa o desempenho, os dados ou a configuração dos serviços essenciais.
2	**Ataques Internos**	• Ataque aos ativos do DataCenter.
3	**Desastres Naturais**	• Descargas elétricas (raios). • Ocorrências sísmicas.
4	**Falha de Conectividade**	• Perda da capacidade de conexão entre a sede do TRT e as demais unidades.
5	**Falha de Hardware**	• Falha que necessite reposição de hardware crítico ou reparo, e cujo reparo ou aquisição dependa de processo licitatório.

6	**Falha Humana**	• Acidente ao manusear equipamentos, ou abastecimento do tanque de combustível.
7	**Falha na Climatização da Sala Cofre**	• Superaquecimento dos ativos devido a falha no dimensionamento de carga na sala cofre. • Falha na unidade de climatização e não emissão de alertas de monitoração.
8	**Incêndio**	• Fogo causado por curto circuito nas instalações.
9	**Indisponibilidade de Backup**	• Cópia de segurança dos dados indisponível ou sem integridade.
10	**Indisponibilidade de Rede/Circuitos**	• Rompimento de fibra óptica decorrente da execução de obras públicas, desastres ou acidentes. • Mal funcionamento de switch gerenciador de segmento de rede. • Interrupção dos serviços de conectividade com as operadoras de telecomunicação por mais de 12 horas.
11	**Interrupção de Energia Elétrica**	• Causada por fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 12 horas. • Causada por fator interno que comprometa a rede elétrica do prédio com curto-circuitos, incêndio e infiltrações. • Impossibilidade de acionar o grupo gerador no momento de uma queda de energia.

6. EQUIPES, PAPÉIS E RESPONSABILIDADES

Considerando que os tratamentos dos eventos de desastre requerem a necessidade de atuação multidisciplinar de vários perfis profissionais, temos que a construção deste plano torna necessário atribuir responsabilidades, componentes e papéis definidos para os grupos de trabalho, que juntos executarão tarefas definidas.

Os grupos aqui definidos podem possuir participantes lotados em várias unidades do organograma da SETIC. Estes componentes podem participar cumulativamente de vários grupos, maximizando a equipe técnica disponível. Os grupos foram classificados de acordo com as suas atribuições, sendo eles:

I. Equipe de Gestão de Continuidade;
II. Equipe de Infraestrutura Computacional e Segurança da Informação;
III. Equipe de Serviços e Software.

6.1. Equipe de Gestão de Continuidade

A Equipe de Gestão de Continuidade será composta pelos membros designados para compor o Comitê de Gestão de Tecnologia da Informação e Comunicação (CGesTIC) e por seus respectivos suplentes.

O papel de líder desta equipe será exercido pelo Secretário de TIC e caberá ao mesmo administrar e manter o Plano de Administração de Crises e acionar os membros da equipe quando necessário.

6.1.1. Responsabilidades:

- Avaliar o Plano de Continuidade de Serviços Essenciais de TIC de forma periódica e decidir pelo seu acionamento quando da ocorrência de desastres, respondendo em nível institucional pela execução do plano e demais ocorrências relacionadas.

- Informar sobre a evolução das providências em andamento, visando restaurar o serviço inoperante junto a servidores, autoridades, fornecedores e Gabinete da Presidência, que se encarregará de prestar informações à mídia, caso necessário.

7.1.2 - PAPÉIS DA EQUIPE DE GESTÃO DE CONTINUIDADE				
#	PAPEL	EXECUTOR	E-MAIL	TELEFONE
1	Secretário de TIC	*	*	*
2	Chefe da Coordenadoria de Infraestrutura e Serviços	*	*	*
3	Chefe da Coordenadoria de Desenvolvimento de Soluções e Aplicações	*	*	*
4	Chefe da Divisão de Governança, Apoio à Gestão de TIC e Iniciativas Nacionais	*	*	*
5	Chefe da Divisão de Segurança da Informação	*	*	*
6	Chefe da Seção de Contratos	*	*	*
7	Chefe da Seção de Infraestrutura Computacional	*	*	*
8	Chefe da Seção de Suporte	*	*	*

* Informação não disponível para essa versão publicada.

6.2. Equipe de Infraestrutura Computacional e Segurança da Informação

O papel de líder desta equipe será exercido pelo Chefe da Coordenadoria de Infraestrutura e Serviços e caberá ao mesmo administrar e manter o Plano de Recuperação de Desastres e acionar os membros da equipe quando necessário.

6.2.1. Responsabilidades

- Responsável pela infraestrutura que abriga os sistemas de TIC e pela garantia que as estruturas alternativas (lógicas ou físicas) são mantidas adequadamente.
- Avaliar os danos e supervisionar a execução do Plano de Recuperação de Desastres.
- Avaliar os danos específicos de qualquer infraestrutura de rede no fornecimento de dados e conectividade de rede de voz, incluindo WAN, LAN e quaisquer conexões de telefonia interna dentro do TRT14 ou de infraestrutura externa junto aos servidores.
- Fornecer a infraestrutura de servidores físicos e virtuais necessária para que a SETIC execute suas operações e processos essenciais durante um desastre.
- Prover mecanismos de segurança no ambiente principal e alternativo.

- Resguardar aplicações e dados, evitando que desdobramentos de segurança afetem o acionamento da continuidade, cuja proteção estará contida na política de segurança.
- Monitoramento e análise da estrutura de redundância.
- Fornecer aos funcionários as ferramentas de que necessitam para desempenhar suas funções da forma mais rápida e eficiente possível. Eles precisarão provisionar os servidores do TRT14 na solução de contingência.
- Monitorar e recuperar as estruturas de armazenamento do BD.
- Responsável por analisar as perdas e mapear a quantidade de dados perdidos, tempo de recuperação desses dados e formular estratégia de recuperação de dados de acordo com as políticas pré-estabelecidas.

7.2.2 - PAPÉIS DA EQUIPE DE INFRAESTRUTURA COMPUTACIONAL E SEGURANÇA DA INFORMAÇÃO				
#	PAPEL	EXECUTOR	E-MAIL	TELEFONE
1	Chefe da Coordenadoria de Infraestrutura e Serviços	*	*	*
2	Chefe da Divisão de Segurança da Informação	*	*	*
3	Chefe da Seção de Banco de Dados	*	*	*
4	Chefe da Seção de Infraestrutura Computacional	*	*	*
5	Chefe da Seção de Redes e Comunicação	*	*	*
6	Chefe da Seção de Suporte	*	*	*

* Informação não disponível para essa versão publicada.

6.3. Equipe de Serviços e Software

O papel de líder desta equipe será exercido pelo gestor responsável pela unidade de Gerenciamento de Serviços e caberá ao mesmo administrar e manter o Plano de Continuidade Operacional e acionar os membros da equipe quando necessário.

6.3.1. Responsabilidade

- Garantir que as aplicações essenciais funcionem como exigido para atender aos objetivos de negócios, durante ocorrência do desastre. Eles serão os principais responsáveis por assegurar e validar o desempenho das aplicações essenciais e podem ajudar outras equipes de TIC, conforme necessário.

7.1.2 - PAPÉIS DA EQUIPE DE SERVIÇOS E SOFTWARE				
#	PAPEL	EXECUTOR	E-MAIL	TELEFONE

3	**Chefe da Coordenadoria de Desenvolvimento de Soluções e Aplicações**	*	*	*
6	**Chefe da Seção de Sistemas Administrativos**	*	*	*
6	**Chefe da Seção de Sistemas Judiciais**	*	*	*
8	**Chefe da Seção de Suporte**	*	*	*

* Informação não disponível para essa versão publicada.

7. ATIVAÇÃO DO PLANO

O Plano de Continuidade de Serviços Essenciais de TIC será ativado quando da ocorrência de algum dos cenários de inoperância ou ocorrência de um risco desconhecido ou caso uma vulnerabilidade tenha grande possibilidade de ser explorada.

O plano também poderá ser invocado em casos de testes ou por determinação da Equipe de Gestão de Continuidade em conjunto com a Alta Administração do TRT14. O acionamento das demais equipes será realizado pelo líder da Equipe de Gestão de Continuidade, de acordo com as características de cada ocorrência, registrando o evento através do formulário “Ativação do Plano de Continuidade de Serviços Essenciais de TIC” onde serão consignadas informações como data de início e fim do incidente, descrição sucinta do ocorrido e quais as equipes acionadas.

Os integrantes das equipes, após acionados, iniciarão a avaliação e investigação do ocorrido, podendo acionar outras equipes caso necessário. Os protocolos e procedimentos de recuperação deverão ser imediatamente iniciados visando cumprir os parâmetros MTPD - Maximum Tolerable Period of Disruption (Período Máximo de Interrupção Tolerável) e RTO - Recovery Time Objective (Tempo Objetivado de Recuperação) definidos no item “Análise de Impacto no Negócio”.

ATIVAÇÃO DO PLANO DE CONTINUIDADE DE SERVIÇOS ESSENCIAIS DE TIC	
Data/Hora de Início:	
Data/Hora do Fim:	
Descrição:	
Equipes Acionadas:	
Resultado:	

8. ANÁLISE DE IMPACTO NO NEGÓCIO

A Análise de Impacto no Negócio é o processo que analisa os componentes de negócio da organização e estimar os impactos que uma interrupção teria sobre eles, permitindo que sejam considerados críticos ou não para a organização e priorizados para as atividades de continuidade. Ela quantifica os impactos da descontinuidade na entrega do serviço, riscos para entrega do serviço e o tempo e o ponto objetivados de recuperação (RTO e RPO). Esses requisitos de recuperação são usados para desenvolver estratégias, soluções e planos.

8.1. Componentes de Negócio Associados

Um componente de negócio é um objeto estratégico ou tático da organização que permite uma visão geral diferenciada dos riscos quando associado a ativos. Os componentes de negócio da camada estratégica representam, em geral, os processos de mais alto nível da organização, ao passo que os componentes da camada tática representam os sistemas e os serviços que suportam os processos. Ele é suportado por um ou mais componentes táticos. Na figura a seguir, estão representados os componentes associados a este plano.

COMPONENTES DE NEGÓCIO ASSOCIADOS							
NOME	**RESPONSÁVEL**	**CRITICIDADE**	**DESCRIÇÃO**	**OMNC**	**RPO**	**RTO**	**MTPD**
Prestação Jurisdicional Trabalhista na 14ª Região	Desembargador Presidente	Muito Alta	Componente de negócio estratégico que representa a missão do Tribunal que é promover justiça por meio da prestação jurisdicional trabalhista célere, eficaz, efetiva e outras ações afirmativas de cidadania.	-	-	-	-
PJE	Secretário de TIC	Muito Alta	Componente de negócio tático que suporta de forma direta a prestação jurisdicional trabalhista.	Garantir a disponibilidade do sistema PJe, não estando disponíveis os sistemas satélites.	24 h	120 h	168 h
PORTAL INSTITUCIONAL	Secretário de TIC	Muito Alta	Componente de negócio tático que suporta de forma direta a prestação jurisdicional trabalhista. No Portal Institucional são disponibilizadas as principais informações sobre processos, seus andamentos e o inteiro teor dos atos judiciais neles praticados, ressalvadas as exceções legais ou regulamentares.	Garantir que os links de acesso ao sistema PJe estejam disponíveis.	24 h	120 h	168 h
SIGEP	Secretário de TIC	Muito Alta	Componente de negócio tático instituído pelo CSJT como solução única e integrada de gestão de pessoas nos Órgãos da Justiça do Trabalho, promovendo a padronização dos processos, garantindo a consistência das informações e aprimorando a eficiência operacional das unidades	Garantir a disponibilidade do sistema SIGEP, não estando disponíveis os sistemas satélites.	24	120 h	168 h

			envolvidas.				
PROAD	Secretário de TIC	Muito Alta	Componente de negócio tático definido como sistema único para tramitação de processos administrativos do Tribunal Regional do Trabalho da 14ª Região. É responsável pela gestão dos processos administrativos de forma eletrônica contemplando todas as fases do processo, da autuação até o seu arquivamento.	Garantir que os links de acesso ao sistema PROAD estejam disponíveis.	24	120 h	168 h
GOOGLE WORKSPACE	Secretário de TIC	Alta	Componente de negócio tático que de comunicação, colaboração e produtividade baseada em nuvem.	Garantir a disponibilidade da ferramenta “Google Workspace”.	24	120 h	168 h
RDP	Secretário de TIC	Alta	Componente de negócio tático que viabiliza o acesso remoto e controlado dos servidores em regime de teletrabalho aos sistemas do Tribunal.	Garantir a disponibilidade e funcionamento da ferramenta “RDP”.	24	120 h	168 h

8.2. Ativos Associados aos Componentes de Negócio Tático

Um ativo é qualquer recurso que tenha valor para a organização e cujos riscos devem ser gerenciados. Já os ativos associados, são todos os ativos tecnológicos que suportam um componente de negócio tático, e que em caso de falha e/ou indisponibilidade parcial ou total, de qualquer um deles ou de todos, podem impactar a continuidade dos serviços essenciais de TIC. A seguir são descritos por componente tático, o conjunto de ativos de tecnologia associados aos mesmos:

ATIVOS ASSOCIADOS AOS COMPONENTES DE NEGÓCIO TÁTICO				
#	**COMPONENTE TÁTICO**	**NOME DO ATIVO**	**DESCRIÇÃO DO ATIVO**	**COMPONENTES DO ATIVO**
1	**********	**********	**********	**********
2	**********	**********	**********	**********
3	**********	**********	**********	**********
N	...			

As informações relativas a esta tabela possuem caráter confidencial, sendo disponibilizadas apenas para as pessoas autorizadas.

8.3. Análise de Riscos de TIC dos Ativos Associados aos Componentes de Negócio

Para evitar que os riscos de TIC, dos ativos associados aos componentes de negócio se materializem e possam impactar a continuidade dos serviços essenciais de TIC e também

permitir às instâncias internas de Governança e Gestão de TIC tomarem decisões estratégicas, táticas e operacionais considerando os riscos tratados, a área de TIC gerencia os riscos de TIC.

O levantamento de informações acerca dos riscos de TIC é realizado através do Processo de Gerenciamento de Riscos de TIC deste Tribunal.

9. ESTRATÉGIAS DE CONTINUIDADE

Para melhor se proteger dos principais riscos, ameaças e cenários de inoperância e reforçar a continuidade dos serviços essenciais de TIC as estratégias de continuidade adotadas pelo Tribunal são: a redundância de ativos de informação, comunicação e energia elétrica e o teletrabalho temporário. As estratégias de continuidade podem ser executadas conjuntamente ou isoladamente, conforme o cenário de inoperância.

Na maioria dos cenários de inoperância a estratégia de redundância será executada de forma automática, nos demais, ocorrerá de forma manual através da execução de procedimentos (ações de contingência e recuperação) que serão detalhados nos planos associados.

A estratégia de teletrabalho temporário será executada, quando houver viabilidade técnica, em cumprimento de determinação superior, quando houver impossibilidade de execução dos serviços essenciais de TIC diretamente no posto de trabalho habitual do usuário interno de TIC. Para viabilização desta estratégia, poderão ser disponibilizados ativos de informação aos usuários internos de TIC necessários para a execução de suas atribuições.

10. PLANOS ASSOCIADOS

O Plano de Continuidade de Serviços Essenciais de TIC é constituído de planos específicos que desdobram e descrevem as ações que serão executadas para assegurar a continuidade dos serviços essenciais de TIC, sendo eles:

- **Plano de Continuidade Operacional (PCO):** Planejamento utilizado para garantir a continuidade dos serviços críticos de TIC na ocorrência de um desastre, enquanto recupera-se o ambiente principal;
- **Plano de Administração de Crise (PAC):** Planejamento utilizado para definir as atividades das equipes envolvidas e gerenciar as ações de contingência e comunicação durante e após a ocorrência de um desastre, com intuito de minimizar impactos, até a superação da crise;
- **Plano de Recuperação de Desastre (PRD):** Planejamento utilizado para recuperar o ambiente principal e retomar seus níveis originais de operação.

10.1 Plano de Continuidade Operacional (PCO)

O PCO descreve os procedimentos necessários para a execução das estratégias de continuidade dos serviços essenciais de TIC, visando garantir a continuidade dos serviços essenciais de TIC na ocorrência de um desastre, enquanto recupera-se o ambiente principal.

É escopo deste plano garantir ações de continuidade durante e depois da ocorrência de uma crise ou cenário de desastre, tratando-se apenas das ações de contingência definidas nas estratégias de continuidade.

Tão logo ocorra um dos cenários de inoperância e o Plano de Continuidade de Serviços Essenciais de TIC seja ativado, o líder da Equipe de Infraestrutura Computacional e Segurança da Informação deve verificar a dimensão do impacto, extensão e possíveis desdobramentos do ocorrido.

As informações devem ser consolidadas e submetidas à Equipe de Gestão de Continuidade para avaliação e decisão sobre a ativação do PCO e início das ações de contingência necessárias para a continuidade dos serviços essenciais de TIC.

Dado o aval pelo Equipe de Gestão de Continuidade para ativação do PCO, os líderes da Equipe de Infraestrutura Computacional e Segurança da Informação e Equipe de Serviços e Software deverão se reunir com os líderes do PRD e PAC com o intuito de coordenar prazos e orquestrar as ações de contingência.

As ações de contingência estão vinculadas à estratégia de continuidade que será executada e à viabilidade técnica.

Uma estratégia de redundância efetiva demanda investimentos financeiros contínuos e escalares. É necessário dispor de ativos replicados (servidores, storages, switches, no-breaks, softwares, links de comunicação e data centers) e também contratos de manutenção. Na maioria dos cenários de inoperância a estratégia de redundância será executada por procedimentos automáticos, sem necessidade de interação humana. Quando não, a redundância ocorrerá de forma manual através da execução de procedimentos que serão detalhados a seguir:

ESTRATÉGIA DE REDUNDÂNCIA			
#	**CENÁRIO DE INOPERÂNCIA**	**ATIVO**	**PROCEDIMENTOS MANUAIS DE REDUNDÂNCIA**
1	**Falha de Hardware**	Storage	• O hardware dos storages foram especificados de forma que serem todos redundantes, sendo que o storage são dimensionados a funcionar com até 50% do hardware (com exceção dos discos) em estado de falha; • Acionar garantia ou suporte.
2	**Falha de Hardware**	Switch Core	**Falha em um nó:** - Acionar a garantia do equipamento e pedir peça de reposição; - Instalar fisicamente o novo módulo; - Restabelecer a pilha com o nó anterior; - Aguardar a ressincronização automática da configuração entre os nós; - Validação da configuração; - Realizar a reconexão dos transceivers e fibras obedecendo a ordem anterior; - Testes e finalização. - Falha na fonte: - Acionar a garantia do equipamento e pedir peça de reposição; - Substituir a fonte do equipamento; - Falha na pilha: - Acionar a garantia do equipamento e pedir peça de reposição; - Remover as ligações de cabos ethernet e fibra óptica do equipamento, mapeando suas respectivas posições; - Substituir o equipamento da sala cofre, recolocando o cabeamento conforme o mapeamento; - Reconfigurar o equipamento através do backup do arquivo de configuração; - Validar as configurações e colocar o equipamento em operação.
3	**Falha de Hardware**	Roteador	**Falha de roteador de borda:**

			- Falha de um nó: - Acionar a garantia do equipamento e pedir peça de reposição; - Verificar a conectividade de todos os links pelo equipamento backup; - Verificar processos e sessões BGP e rotas aprendidas; - Verificar interface VRRP como Running Master na unidade backup; - Realizar a substituição da unidade defeituosa, e restauração do backup a configuração; - Verificar restauração; - Reconexão dos cabos; - Checagem dos processos e sessões BGP e rotas aprendidas; - Verificar a conectividade de todos os links pelo equipamento master. **Falha de todos os nós:** - Migrar as rotas para os roteadores virtuais; - Verificar processos e sessões BGP, rotas aprendidas e conectividade; - Acionar a garantia do equipamento e pedir peça de reposição; - Realizar a substituição da unidade defeituosa, e restauração do backup a configuração; - Verificar restauração; - Reconexão dos cabos; - Checagem dos processos e sessões BGP e rotas aprendidas; - Reestabelecer a rota para as máquinas físicas; - Verificar a conectividade de todos os links pelos equipamentos master e backup. **Falha de roteador concentrador:** **Falha de um nó:** - Acionar a garantia do equipamento e pedir peça de reposição; - Verificar a conectividade de todos os links pelo equipamento backup; - Verificar processos e sessões OSPF e rotas aprendidas; - Verificar interface VRRP como Running Master na unidade backup; - Realizar a substituição da unidade defeituosa, e restauração do backup a configuração; - Verificação da restauração; - Reconexão dos cabos; - Checagem dos processos e sessões BGP e rotas aprendidas; - Verificar a conectividade de todos os links pelo equipamento master. **Falha de todos os nós:** - Migrar as rotas para os roteadores virtuais; - Verificar processos e sessões BGP, rotas aprendidas e conectividade; - Acionar a garantia do equipamento e pedir peça de reposição; - Realizar a substituição da unidade defeituosa, e restauração do backup a configuração;

			- Verificar restauração; - Reconexão dos cabos; - Checagem dos processos e sessões BGP e rotas aprendidas; - Reestabelecer a rota para as máquinas físicas; - Verificar a conectividade de todos os links pelos equipamentos master e backup. **Falha de roteador CPE:** **Falha de um nó:** - Acionar a garantia do equipamento e pedir peça de reposição; - Verificar a conectividade de todos os links pelo equipamento backup; - Verificar processos e sessões OSPF e rotas aprendidas; - Verificar interface VRRP como Running Master na unidade backup; - Realizar a substituição da unidade defeituosa, e restauração do backup a configuração; - Verificação da restauração; - Reconexão dos cabos; - Checagem dos processos e sessões BGP e rotas aprendidas; - Verificar a conectividade de todos os links pelo equipamento master. **Falha de todos os nós:** - Migrar as rotas para os roteadores virtuais; - Verificar processos e sessões BGP, rotas aprendidas e conectividade; - Acionar a garantia do equipamento e pedir peça de reposição; - Realizar a substituição da unidade defeituosa, e restauração do backup a configuração; - Verificar restauração; - Reconexão dos cabos; - Checagem dos processos e sessões BGP e rotas aprendidas; - Reestabelecer a rota para as máquinas físicas; - Verificar a conectividade de todos os links pelos equipamentos master e backup.
4	**Falha de Conectividade**	Link Interior	**Falha de apenas um link:** - Confirmar a indisponibilidade do link e respectivo túnel IPSec; - Verificar a abertura de chamado pelo proativo da operadora. Caso ainda não exista, solicitar o reparo; - Após o reestabelecimento do link, checar a conectividade, o túnel IPSec, e os parâmetros de qualidade. **Falha de todos os links:** - Verificar a instância OSPF nos concentradores em Porto Velho/RO, e as rotas associadas; - Verificar a disponibilidade de energia no local; - Verificar se os roteadores do TRT14 de todas as operadoras da localidade estão energizados e conectados; - Caso toda a infraestrutura esteja funcional, entrar em contato com as operadoras para proceder com investigação do caso e possível reparo; - Informar a localidade da interrupção e prazo para solução;

			- Após retorno da conectividade, realizar os testes de qualidade, túneis IPSec e rotas publicadas.
5	**Falha de Climatização do Data Center**	Data Center	- Ir até o local e verificar quantos equipamentos estão inoperantes; - Entrar em contato com a unidade responsável e solicitar urgência no conserto; - Desligar todas as lâminas e o Chassis, reduzindo a rápida subida de temperatura; - Aguardar uma hora e verificar se a temperatura ficou estabilizada; - Solicitar a engenharia que ligue o ar central de forma emergencial e acionar os botões do quadro de comando que iniciam a circulação de ar através da refrigeração central; - Após o resfriamento do local, religar a Blade e rebalancear as máquinas virtuais; - Revisar o funcionamento da climatização e desligar a refrigeração central através do quadro de comando; - Aguardar uma hora e verificar se a temperatura ficou estabilizada.
6	**Falha de Software**	Máquina Virtual	- No caso de falha no servidor vmware, o gerenciador executará a procedimento de movimentação da máquina para outro virtualizador; - Falha na Máquina Virtual - restaurar a máquina do backup; - Restaurar snapshot caso exista.
7	**Falha de Software**	Banco de Dados	● **Postgres Réplica:** - Realizar a reconfiguração dos datasources dos servidores de aplicação do PJe apontando para o banco de dados máster; - Reiniciar os servidores de aplicação; - Realizar os testes de consultas no sistema.. ● **Postgres Master:** - Transformar o banco de dados de réplica (somente leitura) em máster (leitura e gravação); - Reconfigurar a VM com os recursos computacionais iguais ao do banco master (CPU e memória); - Reconfigurar o IP da VM de réplica com o mesmo do banco master; - Realizar a reconfiguração dos datasources dos servidores de aplicação do PJe apontando todos para o banco de dados máster; - Reiniciar o sistema e validar as configurações. ● **Oracle RAC:** - Transformar o Oracle Dataguard (réplica) em máster (leitura e gravação); - Alterar o IP atribuído ao FQDN utilizado pelas aplicações Oracle para o IP do Dataguard; - Realizar a reconfiguração das aplicações que apontam diretamente para IP do anterior máster, apontando para o Dataguard; - Realizar o reinício das aplicações; - Validar os acessos e sistemas. **Alternativamente:** - Realizar a reinstalação do cluster conforme a documentação do Wiki TI; - Voltar o backup mais recente dos arquivos, seja da área de stage de backup ou diretamente do sistema de backup;

			- Realizar o reinício das aplicações; - Validar os acessos e sistemas.

10.1.1. Estratégia de Teletrabalho Temporário

A estratégia de teletrabalho temporário será executada, desde que haja viabilidade técnica, e em cumprimento de determinação superior, quando da impossibilidade de execução dos serviços essenciais de TIC diretamente do posto de trabalho habitual do usuário interno de TIC, podendo, por determinação superior, serem disponibilizados ativos de informação (estação de trabalho, notebook, monitores) aos usuários internos de TIC.

Os serviços essenciais de TIC que fazem parte do escopo do Plano de Continuidade dos Serviços Essenciais de TIC, são executados através da internet, e o usuário de TIC deverá dispor no local em que realizará o teletrabalho de link de internet adequado e de seus ativos (próprios ou disponibilizados pelo Tribunal). Outras ferramentas e softwares poderão ser disponibilizados pela SETIC, caso haja viabilidade técnica, para permitir de forma restrita ou irrestrita a conectividade com a rede interna do Tribunal e o acesso parcial ou total a outros serviços de TIC.

Após a recuperação do desastre que causou a inoperância e o retorno dos serviços essenciais de TIC à normalidade, o PCO será encerrado e as ações executadas no período relatadas e submetidas à Equipe de Gestão de Continuidade.

10.2. Plano de Administração de Crise (PAC)

Este plano especifica as ações ante os cenários de desastres. As ações incluem gerir, administrar, eliminar ou neutralizar os impactos, inerentes ao relacionamento entre os agentes envolvidos e/ou afetados, até a superação da crise, através da orquestração das ações e de uma comunicação eficaz. O PAC define as atividades das equipes envolvidas e gerencia as ações de contingência e comunicação durante e após a ocorrência de um desastre, tendo como escopo minimizar os impactos, até a superação da crise.

A ativação do plano será feita pela SETIC e tem por objetivo gerenciar e coordenar as providências a serem tomadas no âmbito da continuidade operacional e recuperação do desastre, como também criar um canal de comunicação centralizado com a administração sobre o trabalho realizado até a normalização da situação.

10.2.1. Comunicação da Ocorrência de um Desastre

As recomendações para consecução do plano poderá iniciar através da Comunicação da Ocorrência de um Desastre. Na ocorrência de um desastre faz-se necessário entrar em contato com diversas áreas e partes interessadas, principalmente as afetadas para informá-las de seu efeito na continuidade dos serviços essenciais de TIC e tempo de recuperação. A Equipe de Gestão de Continuidade será responsável por contatar estas unidades e partes interessadas para repassar as informações pertinentes a cada grupo, setor ou segmento. Após reunião com líderes do PRD e PCO, a Equipe de Gestão de Continuidade elaborará um breve programa de comunicação para acionar as partes envolvidas e afetadas, objetivando informar a todos sobre a perspectiva de esforços necessários para o restabelecimento dos serviços. Os itens seguintes, definem os níveis necessários de comunicação:

- **Comunicação com os Usuários Internos de TIC:** A Equipe de Gestão de Continuidade deverá prover um meio de contato específico para este fim, com intuito de que os usuários internos de TIC mantenham-se informados da ocorrência de um desastre e da inatividade dos serviços essenciais de TIC. As informações a serem fornecidas, de forma a padronizar o nível de informação

sobre o evento ocorrido, compreenderão a estimativa de defasagem de atualização das informações que estarão disponíveis, possíveis restrições de acesso quanto a horários ou de performance, quais serviços ainda estão disponíveis e expectativas de conclusão da recuperação durante o desastre.

- **Comunicação com os Usuários Externos, Cidadãos e Mídia:** A Equipe de Gestão de Continuidade em consonância com a Secretaria de Comunicação Social e Eventos Institucionais do TRT14, deverá fornecer informações pertinentes aos usuários externos: advogados, cidadãos e outros órgãos. As atividades a serem desenvolvidas serão de validação da situação ocorrida de acordo com o cenário, e conforme o caso, requerendo publicação da interrupção dos serviços em meios oficiais e de ampla divulgação, com aval da administração da Corte.
- **Comunicação com Unidades do TRT14:** A Equipe de Gestão de Continuidade deverá acionar diretamente às unidades afetadas pelo desastre e fornecer contato, mantendo informado o titular da unidade atingida quanto a natureza, impacto, abrangência da ocorrência, ações de contingência em andamento e dos processos/sistemas e serviços cobertos pelo PCSE-TIC.
- **Comunicação com Fornecedores e Prestadores de Serviço:** No caso de ocorrência de desastre que envolva comprometimento parcial ou total do Data Center, a Equipe de Gestão de Continuidade deverá acionar diretamente os fornecedores e empresas envolvidas, registrando Data/Hora do contato realizado, bem como a pessoa que foi contactada. Para registro deste contato será utilizado a seguinte Lista de Principais Fornecedores:

LISTA DE FORNECEDORES		
#	EMPRESA	CONTATO
1	**********	**********
2	**********	**********
3	**********	**********
N	...	

As informações relativas a esta tabela possuem caráter confidencial, sendo disponibilizadas apenas para as pessoas autorizadas.

10.2.2. Encerramento do PAC

Uma vez validado o funcionamento do retorno dos sistemas essenciais de TIC e estabilidade do datacenter, a Equipe de Gestão de Continuidade entrará em contato com as partes descritas neste plano provendo as informações de retorno das operações com as informações de status dos serviços essenciais de TIC e o PAC será encerrado, relatando-se as atividades necessárias após a ocorrência do desastre como: remanejamento dos canais de informação e a abertura e acompanhamento de chamados correlatos ao ocorrido.

10.3. Plano de Recuperação de Desastre (PRD)

Este plano descreve os cenários de inoperância e seus respectivos procedimentos planejados, definindo as atividades prioritárias para restabelecer o nível de operação dos serviços no ambiente afetado dentro de um prazo tolerável.

O objetivo principal de um Plano de Recuperação de Desastre é assegurar que se possa responder a um desastre ou a inoperância que afetem os serviços essenciais de TIC e minimizar os efeitos e impactos na continuidade do negócio.

É escopo deste plano garantir o retorno das operações do ambiente principal depois da ocorrência de um cenário de inoperância ou um desastre que afetem os serviços essenciais de TIC.

A ativação do presente plano se dará na ocorrência de um dos possíveis cenários de inoperância elencados a seguir, ou ainda por conta de ocorrência de evento ainda não mapeado que tenha gerado interrupção nos serviços essenciais de TIC.

A partir da determinação e levantamento de potenciais riscos frente às possíveis situações que se apresentam dentro do universo da SETIC, procuramos elencar no quadro abaixo os principais incidentes, suas possíveis causas e medidas macro mais adequadas para recuperação destes cenários de inoperância. São eles:

POSSÍVEIS CENÁRIOS DE INOPERÂNCIA			
#	INCIDENTE	CAUSA	PROCEDIMENTOS MACRO DE RECUPERAÇÃO
1	Falha na Alimentação de Energia Elétrica	Externa	• Acionar a Coordenadoria de Serviços, Infraestrutura e Logística para acionamento junto à prestadora de energia elétrica de solicitação de restabelecimento dos serviços elétricos; • Solicitação de previsão de conclusão das providências.
		Interna	• Acionar a Coordenadoria de Serviços, Infraestrutura e Logística para verificação dos geradores emergenciais; • Acionar a Coordenadoria de Serviços, Infraestrutura e Logística solicitando verificação de cabeamento elétrico, disjuntores, fusíveis, etc, considerando os 2 circuitos independentes (Sala/Ar condicionado).
		Danos na fonte de alimentação ininterrupta	• Solicitar à Coordenadoria de Serviços, Infraestrutura e Logística a manutenção do mesmo e execução de reparos (limpeza, trocas de baterias, conserto de placa, etc).
2	Falha na Refrigeração da Sala Cofre	Falha na alimentação de energia elétrica	• Acionar a Coordenadoria de Serviços, Infraestrutura e Logística para avaliação e reparos; • Solicitar previsão para término dos reparos.
		Falha no equipamento de ar condicionado	• Acionar a Coordenadoria de Serviços, Infraestrutura e Logística para avaliação e reparos; • Solicitar previsão para término dos reparos.

3	Malware	Infecção do equipamento por acesso a sítio malicioso ou arquivo infectado	• Fazer atualização e varredura de antivírus e identificar os meios que possibilitaram a contaminação; • Descontaminar equipamento com as ferramentas apropriadas; • Verificação e reconfiguração da estação de trabalho, se for o caso; • Medidas de conscientização quanto a política de segurança da informação para os usuários envolvidos; • Testes.
4	Indisponibilidade dos Serviços / Aplicações pela Rede Interna	Danos ao Switch	• Verificação de cabeamento estruturado e/ou fibra óptica; • Verificar a alimentação elétrica; • Verificação quanto a existência de equipamento reserva; • Acionar a garantia, se for o caso; • Reconfiguração do novo equipamento através da biblioteca de configurações; • Instalar e testar equipamento.
		Danos ao Cabeamento	• Substituir ou reparar o cabo danificado; • Verificação de segmento/porta lógica para uma via de conexão alternativa.
		Danos ao Servidor de Arquivos / Aplicação	• Verificação de montagem de máquina virtual ou disponibilidade de equipamento reserva; • Acionar a garantia, se for o caso; • Identificação do backup de dados mais recente e restauração das informações; • Ativação do equipamento em produção, baseado na biblioteca de configurações; • Testes.
		Danos ao Servidor de Autenticação	• Verificação de montagem de máquina virtual ou disponibilidade de equipamento reserva; • Acionar a garantia, se for o caso; • Identificação do backup de dados mais recente e restauração das informações; • Ativação do equipamento em produção, baseado na biblioteca de configurações; • Testes.
		Danos na Estação de Trabalho	• Verificação da existência de equipamento de contingência; • Acionar a garantia, se for o caso; • Restaurar imagem do equipamento de acordo com a biblioteca de configurações; • Testes.
		Remoção de Dados pelo Usuário	• Identificar meios pelos quais foram possíveis se fazer a remoção e tratá-los em conformidade com a Política de Segurança da Informação adotada; • Identificação do backup de dados mais recente e restaurar as informações removidas;

			• Restauração do backup; • Testes.
5	Indisponibilidade dos Serviços de Internet	Servidor Internet Indisponível	• Abrir chamado Service Desk; • Verificar configurações e conteúdos WEB; • Recomposição de rotinas dos serviços, se for o caso; • Testes.
		Link Internet Indisponível	• Abrir chamado Service Desk; • Verificar configurações e conteúdos WEB; • Recomposição de rotinas dos serviços, se for o caso; • Testes.
		Estação de Trabalho Desconfigurada	• Reconfiguração segundo política de acesso; • Verificação do perfil de usuário, se for o caso; • Testes.
6	Indisponibilidade de Links de Comunicação com as unidades do Interior	Rompimento de Fibras/Cabos e Outras	• Verificação de infraestrutura interna e nas unidades do Interior; • Abrir chamado no Service Desk da concessionária dos Links de comunicação; • Monitoramento do SLA acordado.
7	Indisponibilidade de Restauração de Backups	Mídia Indisponível	• Verificação da disponibilidade de mídia alternativa; • Identificação do backup de dados mais recente e restauração das informações, se for o caso; • Verificar causas de indisponibilidade e revisar processo de execução; • Testes.
		Backup mais Recente Inexistente	• Verificar existência de backup anterior; • Recomendar ao usuário a inclusão de seus arquivos no drive compartilhado em nuvem.

10.3.1. Procedimentos de Recuperação

Os procedimentos macro de recuperação elencados na tabela acima, serão conduzidos pela execução formal das seguintes etapas definidas abaixo sob a supervisão da Equipe de Infraestrutura Computacional e Segurança da Informação:

- I**dentificação de Ativos Inoperantes:** A Equipe de Infraestrutura Computacional e Segurança da Informação deverá identificar e listar todos os Ativos/Serviços inoperantes em decorrência do desastre. As informações de cada ativo inoperante devem ser condensadas num levantamento contendo no mínimo identificação, IP, breve descrição de sua função, indicação se está em período de garantia, se há redundância física disponível, responsável, fornecedor.
- **Identificação de Acessos Interrompidos:** A Equipe de Infraestrutura Computacional e Segurança da Informação deverá identificar a existência de interrupções de conexões e acessos gerados após o desastre, informando sua abrangência (rede local, rede WAN ou provedor de serviços), quando aplicável.

- **Identificação de Serviços Descontinuados:** A Equipe de Infraestrutura Computacional e Segurança da Informação deverá mapear quais serviços foram descontinuados contendo as informações de perda de ativo e de conexão com intuito de levar ao conhecimento da Equipe de Gestão de Continuidade. O relatório deverá abranger todos os componentes necessários à plena operação da aplicação como servidores, máquinas virtuais, banco de dados, firewall, storage, routers e switches, bem como respectivas configurações de proxy, DNS, rotas, vlans, etc.
- **Elaboração de Cronograma de Recuperação:** A Equipe de Infraestrutura Computacional e Segurança da Informação após o mapeamento das perdas e impactos elaborará um breve cronograma de recuperação dos serviços/aplicações atingidos pelo desastre.
- **Substituição de Ativos e Equipamentos:** Em caso de perda de ativos, deverá ser imediatamente informado à Equipe de Gestão de Continuidade, a necessidade de aquisição de ativos perdidos que não puderem ser recuperados. A equipe irá mensurar quanto tempo a aquisição irá impactar o RTO de cada serviço, comunicando a Equipe de Gestão de Continuidade se há alguma solução alternativa a ser tomada enquanto é realizada a aquisição. A equipe deve verificar dentre os ativos danificados, quais estão cobertos por garantia e se a mesma poderá ser acionada neste caso através da lista de fornecedores. As informações pertinentes à alteração do tempo de recuperação dos serviços serão repassadas às equipes do PCO e PAC.
- **Reconfiguração de Ativos e Equipamentos:** A Equipe de Infraestrutura Computacional e Segurança da Informação deverá verificar se as configurações dos ativos reparados ou substituídos, estão em funcionamento pleno. Caso não estejam, prover cronograma estimado para configurar estes ativos informando a Equipe de Gestão de Continuidade.
- **Teste de Ambiente/Homologação:** O ambiente principal do datacenter deverá ser testado antes do recovery dos dados do backup, no intuito de garantir que o processo de recuperação ocorra conforme o planejado. Os testes incluem:
  - Avaliar a performance para garantir os mesmos níveis de capacidade e disponibilidade dos serviços essenciais, antes do desastre;
  - Validar as configurações.
- **Recuperar dados do backup:** Nos casos de recuperação de dados para as aplicações, este será realizado pela Equipe de Infraestrutura Computacional e Segurança da Informação com a cópia de segurança mais recente disponível, notificando o líder do PRD da data e hora do mesmo.

Ao término do procedimento de recuperação, as informações da recuperação dos serviços serão consolidadas em parecer específico informando horário de restabelecimento de cada serviço, equipamentos adquiridos quando couber, procedimentos de recuperação realizados e fornecedores acionados.

11. VALIDAÇÃO E TESTE DO PLANO DE CONTINUIDADE DOS SERVIÇOS ESSENCIAIS DE TIC

Cumprindo o propósito de reavaliar os procedimentos planejados e com o objetivo de promover a melhoria contínua, este plano será testado e validado em reunião entre os líderes de cada plano associado de acordo com a periodicidade anual ou ainda, mediante necessidade apontada nas reuniões do CGesTIC.

A execução dos passos planejados deve ser registrada indicando: “Data de Execução”, “Tipo do Teste”, “Descrição de Motivo” e “Status”, respeitando ainda os seguintes critérios a serem informados no registro:

11.1. Tipos de testes a serem realizados:

- **Teste de mesa:** o Teste de complexidade simples, no qual é realizada uma análise (crítica ensaios de execução), dos procedimentos e informações descritas, com o objetivo de atualizar e (ou) validar os procedimentos e as informações contidas no plano;
- **Simulação no ambiente:** Simular uma situação real de interrupção. O Teste de complexidade média no qual uma situação “artificial” é criada, por exemplo, é realizada a parada de um processo em horários diferentes das operações diárias (finais de semana, após expediente, etc.) sendo o resultado utilizado para validar se os planos possuem as informações necessárias e suficientes, de forma a permitir recuperação de determinado arranjo de contingência ou processo com sucesso;

Os testes poderão admitir os seguintes status: Programado, Executado, Planejado e Agendado.

O modelo de tabela abaixo servirá como base para registro dos testes deste plano.

REGISTROS DE VALIDAÇÃO E TESTES						
TIPO DE TESTE	DESCRIÇÃO	STATUS	DATA	EXECUTADO POR	OBSERVAÇÃO	RESULTADO

12. ATUALIZAÇÃO DA NORMA

Esta norma será atualizada em conjunto com a revisão da Política de Segurança da Informação ou a qualquer tempo, quando assim recomendado pelo Comitê de Segurança da Informação.