PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DO PARÁ
Gabinete da Presidência

PORTARIA Nº 4592, DE 30 DE SETEMBRO DE 2024.

Institui a Política de Segurança da Informação do Poder Judiciário do Estado do Pará.

A Excelentíssima Senhora Desembargadora **MARIA DE NAZARÉ SILVA GOUVEIA DOS SANTOS**, Presidente do Tribunal de Justiça do Estado do Pará, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a autonomia administrativa atribuída ao Poder Judiciário, conforme prevê o art. 99 da Constituição Federal e o art. 148 da Constituição Estadual;

CONSIDERANDO os termos da Resolução CNJ nº 370/2021, que estabeleceu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), com diretrizes para sua governança, gestão e infraestrutura;

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

CONSIDERANDO a Portaria nº 162/2021, do Conselho Nacional de Justiça-CNJ, que aprovou os Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Norma Técnica ABNT ISO/IEC 27001:2022, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização;

CONSIDERANDO a Norma Técnica ABNT ISO/IEC 27002:2022, que estabelece um código de prática para controles de segurança da informação;

CONSIDERANDO a Norma Técnica ABNT ISO/IEC 27005:2022, que fornece diretrizes para o processo de Gestão de Riscos de Segurança da Informação;

CONSIDERANDO a Norma Complementar nº 04/IN01/DSIC/GSIPR, que estabelece as diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) nos órgãos e entidades da Administração Pública Federal;

CONSIDERANDO a Norma Complementar nº 08/IN01/DSIC/GSIPR, que estabelece as diretrizes para gerenciamento de incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal;

CONSIDERANDO a Norma Complementar no 21/IN01/DSIC/GSIPR, 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;

CONSIDERANDO que é imprescindível garantir a segurança cibernética e a privacidade dos dados tratados no âmbito do Tribunal de Justiça do Estado do Pará, diante da crescente complexidade e diversidade de incidentes cibernéticos no ambiente da rede mundial de computadores;

CONSIDERANDO a necessidade de atualizar os normativos de segurança da informação do Poder Judiciário do Estado do Pará, com o objetivo de atender às reais necessidades em segurança da informação e segurança cibernética, visando à prestação jurisdicional e à credibilidade perante a sociedade paraense;

CONSIDERANDO a necessidade de conscientizar, a nível institucional, todos os usuários do Tribunal de Justiça do Estado do Pará, incluindo magistrados (as), servidores (as), terceirizados (as) e colaboradores (as) em geral, sobre o seu papel na garantia da segurança cibernética e proteção dos dados do Poder Judiciário do Estado do Pará;

RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação do Poder Judiciário do Estado do Pará (PSI-PJPA).

CAPÍTULO I

GLOSSÁRIO

Art. 2º Para os fins desta Portaria, considera-se:

I – Acesso Privilegiado: acesso realizado através de contas com alto nível de privilégio, tendo a possibilidade de realizar alterações nas configurações dos recursos de TIC acessados, instalar softwares e acessar dados confidenciais;

II – Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

III – Análise de riscos: processo para compreender a natureza do risco e determinar o nível de risco;

III – Análise de riscos: processo para compreender a natureza do risco e determinar o nível de risco;

IV – Ativo: qualquer objeto que represente valor para o Poder Judiciário do Estado do Pará como, por exemplo, a informação.

V – Autenticação: processo de identificação das partes envolvidas em um processo;

VI – Autorização: processo que visa garantir que as informações são acessíveis excluivamente àqueles com permissão de acesso;

VII – 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;

VIII – *Backup*: processo de cópia de dados de uma estação de trabalho, servidor ou sistema para armazenar em um local distinto, visando à recuperação em caso de exclusão acidental ou intencional;

IX – Dispositivo Móvel Corporativo: notebooks, smartphones, tablets e similares distribuídos pela Secretaria de Informática, para uso exclusivo por parte de magistrados (as) e servidores (as) do Tribunal;

X – Dispositivo Móvel Particular: notebooks, smartphones, tablets e similares de uso próprio de magistrados (as) e servidores (as) do Tribunal, que não tenham sido distribuídos pela Secretaria de Informática;

XI – Dispositivo Móvel Visitante: notebooks, smartphones, tablets e similares que sejam de pessoas externas e que estejam temporariamente no Tribunal, como usuários (as) dos serviços institucionais ofertados pelo PJPA, prestadores (as) de serviços, dentre outros;

XII – Estabelecimento do contexto: todas as informações da organização que sejam relevantes para a implantação de uma gestão de riscos de segurança da informação;

XIII – ETIR: sigla para Equipe de Tratamento e Resposta a Incidentes de Segurança, denominação tradicionalmente atribuída a um grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança.

XIV – Evento de segurança: ocorrência observável em um ativo e que se relaciona com a segurança da informação ou cibernética do Tribunal;

XV – Gestão de Riscos de Segurança da Informação: conjunto de processos que permite identificar e implementar as medidas de proteção, necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e para equilibrá-los com os custos operacionais e financeiros envolvidos;

XVI – Gestores de Processos, Serviços e Ativos de TIC: responsáveis pelos processos de trabalho, projetos e ações desenvolvidos nos níveis estratégico, tático e operacional do Tribunal;

XVII – Gestores de Riscos: são os titulares das unidades responsáveis pelos serviços, atuando em seu respectivo escopo de trabalho;

XVIII – Identificação de Riscos: processo para localizar, listar e caracterizar elementos do risco;

XIX – Incidente de segurança: evento identificado em um ativo que possa indicar uma possível violação da política de segurança, falhas em processos ou procedimentos de segurança, a exploração de uma vulnerabilidade ou uma situação desconhecida e que se mostra relevante para a segurança da informação ou cibernética do Tribunal;

XX – Medidas de contenção: ações a serem tomadas para impedir o início ou o aumento de danos causados por um determinado incidente em um determinado momento, além de restabelecer o sistema/serviço afetado, de maneira total ou parcial;

XXI – Medidas de erradicação: ações a serem tomadas para solucionar vulnerabilidades e eliminar a causa-raiz de incidentes de segurança;

XXII – Medidas de recuperação: ações a serem tomadas para reestabelecer o ambiente computacional do Tribunal ao último estado válido anterior ao incidente, além de observar a possibilidade de melhorias nas políticas, processos e procedimentos utilizados na gestão de incidentes;

XXIII – *Multifactor Authentication* (MFA): utilização de dois ou mais fatores de autenticação para conceder acesso a um sistema;

XXIV – Privilégio Mínimo: atribuição apenas dos privilégios necessários para o desempenho de uma função ou papel específico;

XXV – Procedimento: conjunto de ações sequenciadas e ordenadas para o atingimento de um determinado fim;

XXVI – Recursos de TIC: recursos que processam, armazenam ou transmitem informações, tais como aplicações, sistemas de informação, computadores, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura, dentre outros;

XXVII – Risco: evento capaz de afetar negativamente os objetivos da organização nos níveis estratégico, tático e operacional;

XXVIII – *Role-based Access Control* (RBAC): método de controle de acesso que atribui permissões aos usuários (as) com base em sua função na organização;

XXIX – *Scan*: ação de varredura executada em um recurso de TIC com o objetivo de detectar e identificar vulnerabilidades existentes;

XXX – Segurança Cibernética: ações que visam proteger a informação armazenada em meios digitais e transmitida através de redes de comunicação, sendo um componente da Segurança da Informação;

XXXI – Segurança da Informação: ações mais amplas que objetivam viabilizar e assegurar a confidencialidade, integridade, disponibilidade e autenticidade das informações, cuidando da redução de riscos no transporte de dados por qualquer meio, digital ou não;

XXXII – Servidores de Aplicação: infraestrutura física ou virtual utilizada para hospedar aplicações acessadas através da rede de dados do Tribunal;

XXXIII – Sistema de Gestão de Segurança da Informação (SGSI): políticas, procedimentos, manuais e recursos associados e atividades coletivamente gerenciadas por uma organização, na busca de proteger seus ativos de informação;

XXXIV – Tratamento de Riscos: processo e ações a serem tomadas para evitar, reduzir, reter ou transferir um risco;

XXXV – Usuários: magistrados (as), servidores (as), terceirizados (as), estagiários (as) e colaboradores (as) em geral;

XXXVI – Vulnerabilidades: conjunto de fatores internos ou causa potencial de um incidente indesejado ,que pode resultar em risco para um sistema ou organização, o qual pode ser evitado por uma ação interna de segurança cibernética ou segurança da informação.

CAPÍTULO II

DIRETRIZES GERAIS

Art. 3º Esta Política visa atender a necessidade de serem estabelecidos mecanismos e diretrizes de controle e proteção dos recursos, processos, serviços de TIC e afins, buscando a confidencialidade, integridade e disponibilidade das informações tratadas no ambiente computacional do Poder Judiciário do Estado do Pará.

Art. 4º Esta Política deve ser parte integrante de todos os instrumentos contratuais que envolvam manipulação de ativos institucionais e deve ser observada por todos os fornecedores (as) com os quais o Tribunal possua contrato.

Art. 5º Os recursos de TIC do Poder Judiciário do Estado do Pará devem ser utilizados de forma adequada e exclusivamente em atividades relacionadas às funções institucionais do usuário que está utilizando o recurso em questão.

Art. 6º Os recursos de TIC do Poder Judiciário do Estado do Pará devem ser monitorados pela Secretaria de Informática e receberão o grau de proteção adequado ao seu nível de criticidade, visando a continuidade da prestação jurisdicional.

Art. 7º O Poder Judiciário do Estado do Pará deve garantir o estabelecimento de controles de identidade e acesso aos recursos de TIC, sendo que estes controles devem ser revisados, modificados ou revogados em caso de alteração ou encerramento das atividades do usuário junto ao Tribunal, ou sempre que for julgado necessário pela Secretaria de Informática ou pelo Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA).

Art. 8º Em caso de suspeita de incidente de segurança envolvendo recursos de TIC do Poder Judiciário do Estado do Pará ou de descumprimento da Política de Segurança da Informação do Poder Judiciário do Estado do Pará (PSI-PJPA), o Gestor de Segurança da Informação deve ser informado através de canal oficial, a ser definido pelo Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA), o qual será amplamente divulgado após sua definição.

CAPÍTULO III

SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 9º O Poder Judiciário do Estado do Pará deverá estabelecer um Sistema de Gestão de Segurança da Informação (SGSI) com as políticas, normas, processos e

procedimentos necessários para elevar sua maturidade em segurança da informação e segurança cibernética. O SGSI será coordenado pelo Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA) e conterá, no mínimo e não se limitando a estes:

I – Normas para Gestão de Riscos de Segurança da Informação;

II – Normas para Gestão de Incidentes de Segurança Cibernética;

III – Normas para Educação e Cultura em Segurança Cibernética;

IV – Normas de Gestão de Acessos para Usuários;

V – Normas para Gestão de Vulnerabilidades;

VI – Normas de Segurança para Teletrabalho;

VII - Normas para Uso de Dispositivos Móveis;

VIII – Normas para Backup e Restauração de Dados.

Art. 10. A Secretaria de Informática deve, através de um portal de governança, disponibilizar as políticas, normas e processos que compõem o Sistema de Gestão de Segurança da Informação (SGSI).

SEÇÃO I

NORMAS PARA GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Art. 11. Estas normas visam estabelecer um processo de Gestão de Riscos de Segurança da Informação a ser utilizado no âmbito do Poder Judiciário do Estado do Pará, nas atividades em que for pertinente o seu uso.

Art. 12. As normas para Gestão de Riscos de Segurança da Informação possuem como objetivos:

I – Implantar uma cultura proativa de gerenciamento de riscos;

II – Apoiar as unidades organizacionais do Poder Judiciário do Estado do Pará no que diz respeito aos riscos de segurança da informação;

III – Aprimorar o processo decisório no âmbito do Tribunal, incorporando a visão de gestão de riscos nas melhores práticas adotadas;

IV – Justificar decisões dos gestores de riscos sobre ações tomadas para mitigar ou assumir riscos;

V – Identificar, avaliar e reagir às oportunidades e ameaças existentes.

Art. 13. O Poder Judiciário do Estado do Pará deverá prover os recursos que se fizerem necessários para a execução desta Política.

Art. 14. A Norma de Gestão de Riscos de Segurança da Informação do Poder Judiciário do Estado do Pará (PGRSI-PJPA) deve estabelecer uma estrutura de gestão de riscos de segurança da informação, que será composta pelo Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA), pela Secretaria de Informática, pela Secretaria de Auditoria Interna, pelos gestores de riscos e pelos gestores de processos, serviços e ativos de TIC.

Parágrafo único. A estrutura de gestão de riscos de segurança da informação, mesmo com papéis e responsabilidades definidos, é de responsabilidade de todos os usuários dos recursos de TIC do Tribunal.

Art. 15. Compete ao Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA), não se limitando a estes:

I – Aprovar a Norma de Gestão de Riscos de Segurança da Informação do Poder Judiciário do Estado do Pará (PGRSI-PJPA);

II – Decidir sobre a prioridade referente aos riscos, quando for necessário;

III – Analisar sobre etapas da Gestão de Riscos que não foram executadas, bem como decidir sobre as providências necessárias a serem tomadas.

Art. 16. Compete à Secretaria de Informática:

I – Disseminar as Normas de Gestão de Riscos de Segurança da Informação do Poder Judiciário do Estado do Pará (PGRSI-PJPA) para todas as unidades que a compõe;

II – Monitorar, avaliar, revisar e propor alterações ou atualizações nestas Normas;

III – Monitorar o tratamento de riscos executado;

IV – Analisar e encaminhar os riscos não tratados para o Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA).

V – Monitorar o processo de gestão de riscos de segurança da informação;

VI – Elaborar relatórios de riscos de segurança de forma periódica e sempre quando for demandado.

Art. 17. Compete aos Gestores de Riscos:

I – Escolher os processos cujos riscos devam ser gerenciados e tratados, baseados em seu nível de criticidade e na dimensão dos prejuízos que podem causar, caso não sejam tratados;

II – Propor níveis aceitáveis de exposição ao risco, de modo a consolidar a tolerância ao risco das unidades e dos serviços auxiliares do órgão;

III – Definir as ações de tratamento a serem implementadas, bem como o prazo de implementação e avaliação dos resultados obtidos.

Art. 18. Compete aos gestores de processos, serviços e ativos de TIC:

I – Contribuir para as atividades de análise e avaliação dos riscos referentes aos processos de trabalho, serviços e ativos de TIC sob sua responsabilidade;

II – Gerenciar os riscos inerentes aos processos de trabalho, serviços e ativos de TIC sob sua responsabilidade, de forma a mantê-los em nível de exposição aceitável;

III – Implementar os planos de ação definidos para tratamento dos riscos referentes aos processos de trabalho, serviços e ativos de TIC sob sua responsabilidade;

IV – Comunicar novos riscos referentes aos seus processos e que não fazem parte da relação de riscos institucionais já identificados.

Art. 19. Estas Normas devem estabelecer um processo de gestão de riscos de segurança da informação que contemple as fases de:

I – Estabelecimento do contexto;

II – Identificação dos riscos;

III – Análise dos riscos;

IV – Avaliação dos riscos;

V – Tratamento dos riscos;

VI – Monitoramento e análise crítica;

VII – Comunicação dos riscos.

§ 1º O Plano de Tratamento de Riscos deve contemplar as iniciativas propostas e os respectivos responsáveis pela implementação destas iniciativas, além do levantamento de recursos necessários e o cronograma para execução das iniciativas de tratamento dos riscos.

§ 2º O Tribunal deve implantar a execução das fases, procedimentos e instrumentos necessários em uma ferramenta de gestão de riscos adequada para o cumprimento do processo.

Art. 20. Os serviços e ativos em funcionamento no ambiente computacional do Tribunal, e os novos a serem homologados, devem ser submetidos à Secretaria de Informática, para que se proceda a execução do processo de gestão de riscos antes da disponibilização para uso por parte dos usuários, visando a prevenção de vulnerabilidades a serem expostas.

Art. 21. Para realização da categorização e classificação de riscos internos e externos, deve ser utilizada uma abordagem qualitativa, medindo o impacto e a probabilidade de ocorrência dos riscos com as seguintes categorias:

I – Muito baixo;

II – Baixo;

III – Médio;

IV – Alto;

V – Muito alto.

Art. 22. O acompanhamento da execução de todas as fases do processo de Gestão de Riscos será realizado pela Secretaria de Informática, em conjunto com o Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA), a Secretaria de Auditoria Interna e o Departamento de Planejamento, Gestão e Estatística, com a devida comunicação a todas as partes interessadas.

Art. 23. O Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA), juntamente com a Secretaria de Auditoria Interna, devem avaliar a política, o processo e os procedimentos de Gestão de Riscos de Segurança da Informação existentes, juntamente com o histórico e os indicadores disponíveis, visando avaliar a possibilidade de melhorias e implementar as medidas necessidades.

SEÇÃO II

NORMAS PARA GESTÃO DE INCIDENTES EM SEGURANÇA CIBERNÉTICA

Art. 24. Estas normas visam definir diretrizes para o estabelecimento de práticas de Gestão de Incidentes de Segurança Cibernética, no âmbito do Poder Judiciário do Estado do Pará

Art. 25. As Normas para Gestão de Incidentes de Segurança Cibernética possuem como objetivo assegurar a identificação, o registro, a avaliação e a priorização de incidentes de segurança cibernética, além de garantir medidas adequadas de contenção, erradicação e recuperação e geração de conhecimento através de lições aprendidas com os referidos incidentes.

Art. 26. Serão alvos das Normas para Gestão de Incidentes de Segurança Cibernética:

I – Eventos de segurança, tanto suspeitos como confirmados, que possam comprometer os ativos que compõem o parque computacional do Tribunal, ou mesmo, interromper a prestação jurisdicional, de forma total ou parcial;

II – Vulnerabilidades de segurança detectadas nos ativos que compõem o parque computacional do Tribunal;

III – Ações realizadas pelos usuários dos recursos de TIC, que possam ir contra a Política de Segurança da Informação do Poder Judiciário do Estado do Pará (PSI-PJPA) e qualquer um de seus anexos;

IV – Alterações indevidas, vazamento ou destruição de dados no âmbito do Poder Judiciário do Estado do Pará.

Art. 27. A Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) será responsável pelo desenvolvimento de um processo para realizar a gestão de incidentes de segurança cibernética do Poder Judiciário do Estado do Pará (PJPA). Este processo deve conter, no mínimo, as seguintes fases:

I – Preparação;

II – Detecção e análise;

III – Contenção, erradicação e recuperação;

IV – Atividades pós-incidente.

§ 1º A fase de preparação consiste em atividades proativas que tenham o objetivo de mapear e proteger o parque computacional do Tribunal, desenvolver e implantar mecanismos para detecção de incidentes e planos de resposta para esses incidentes detectados.

§ 2º A fase de detecção e análise compreende a consolidação de informações sobre eventos suspeitos e a análise destes eventos para a confirmação de que sejam maliciosos, além da avaliação da abrangência e do impacto e a estratégia de comunicação deste evento para as partes interessadas.

§ 3º A fase de contenção, erradicação e recuperação diz respeito a atividades necessárias para conter, de forma imediata, os efeitos de um incidente no parque computacional do Tribunal, erradicação desse incidente e recuperação do ambiente de TIC, caso este tenha sofrido danos por conta do incidente.

§ 4º As atividades pós-incidente visam, após o encerramento do incidente, o aperfeiçoamento dos planos e processos desenvolvidos nas fases anteriores para realizar a melhoria contínua da gestão de incidentes no âmbito do Poder Judiciário do Estado do Pará.

Art. 28. Os incidentes devem ser registrados de forma adequada, com o objetivo de criar um histórico e auxiliar na geração de indicadores que possam subsidiar decisões estratégicas.

Art. 29. Os usuários dos recursos de TIC do Tribunal e as coordenadorias da Secretaria de Informática que são responsáveis pelo gerenciamento dos ativos que compõem o parque computacional do Tribunal, caso tenham alguma suspeita sobre a possibilidade de um incidente, devem notificá-lo, de forma mais breve possível, sem a necessidade de autorização da chefia imediata.

§ 1º A notificação pode ser realizada através de abertura de chamado na Central de Serviços, por e-mail para os endereços etir@tjpa.jus.br e seginfo@tjpa.jus.br, ou diretamente na Secretaria de Informática.

Art. 30. Caso seja confirmado um incidente em algum ativo, esse ativo não deve ser utilizado pelos usuários de TIC e pelos integrantes da SECINFO, sob risco de danos ao ativo e comprometimento da prestação jurisdicional.

Art. 31. O Poder Judiciário do Estado do Pará poderá compartilhar (enviar e receber) informações sobre incidentes de segurança cibernética com:

I – ETIRs que façam parte da Rede de Cooperação do Judiciário;

II – ETIRs de outros órgãos da Administração Pública Federal, Estadual e Municipal;

III – ETIRs de outras entidades públicas e privadas.

§ 1º Apenas serão compartilhadas informações que não comprometam a segurança dos dados e dos ativos do Poder Judiciário do Estado do Pará.

Art. 32. A Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR), com apoio da Secretaria de Informática, será responsável pela condução da análise do incidente, da coleta dos dados necessários, das medidas de contenção, erradicação e recuperação e da comunicação com as partes interessadas.

Art. 33. Quando necessário, a coleta de evidências dos incidentes deve ser realizada pela Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR).

§ 1º Caso a ETIR não detenha as competências necessárias para tal atividade, a coleta pode ser realizada por outra equipe que a detenha, seja interna ou externa, cabendo a ETIR acompanhar a atividade.

Art. 34. Quando o incidente decorrer de suspeita de descumprimento da Política de Segurança da Informação do Poder Judiciário do Estado do Pará (PSI-PJPA), será observado o sigilo durante todo o processo, ficando as evidências, informações e demais registros restritos aos envolvidos na investigação.

Art. 35. O encerramento do incidente será realizado pela Secretaria de Informática, em conjunto com o Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA), com a devida comunicação a todas as partes interessadas.

Art. 36. Após o encerramento do incidente, a Secretaria de Informática, em conjunto com o Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA), deve avaliar as normas, bem como processos e procedimentos de Gestão de Incidentes existentes, juntamente com o histórico e os

indicadores disponíveis, visando avaliar a possibilidade de melhorias e implementar as medidas necessárias.

SEÇÃO III

NORMAS PARA EDUCAÇÃO E CULTURA EM SEGURANÇA CIBERNÉTICA

Art. 37. As Normas para Educação e Cultura em Segurança Cibernética possuem os propósitos de estabelecer, desenvolver e fortalecer a educação e a conscientização dos usuários dos recursos de Tecnologia da Informação e Comunicação (TIC) do Tribunal de Justiça do Estado do Pará, bem como fomentar uma cultura baseada no aprimoramento, no desenvolvimento e na disseminação de conhecimentos e inovações, tanto por parte dos profissionais de tecnologia da informação, quanto por parte dos usuários internos.

Art. 38. São objetivos das Normas para Educação e Cultura em Segurança Cibernética, não se limitando a estes:

I – Propiciar o constante aprimoramento dos níveis de segurança cibernética nos ativos e serviços de Tecnologia da Informação e Comunicação (TIC) do Poder Judiciário do Estado do Pará;

II – Tratar a segurança cibernética como tópico estratégico a ser inserido nas pautas institucionais do Poder Judiciário do Estado do Pará;

III – Elevar a consciência e promover uma cultura baseada em segurança cibernética no âmbito do Poder Judiciário do Estado do Pará;

IV – Assegurar que os usuários compreendam seus papéis na proteção do ambiente e dos dados tratados no âmbito do Poder Judiciário do Estado do Pará;

V – Assegurar a crescente e permanente qualificação, em nível institucional, no tema de segurança cibernética.

VI – Assegurar a crescente e permanente qualificação específica para analistas judiciários e auxiliares judiciários lotados na Secretaria de Informática.

Art. 39. As Normas para Educação e Cultura em Segurança Cibernética do Poder Judiciário do Estado do Pará (PECSC-PJPA) devem desenvolver e elevar a educação e a conscientização dos usuários e profissionais de tecnologia da informação sobre os seguintes assuntos, atinentes ao tema de segurança cibernética, não se limitando a estes:

I – Segurança da Informação, em termos gerais;

II – Segurança física e proteção de dados pessoais e institucionais;

III – Segurança física e proteção de ativos de tecnologia da informação, em termos gerais;

IV – Ações destinadas a garantir a confidencialidade, integridade, disponibilidade e autenticidade dos dados e informações no âmbito do Poder Judiciário do Estado do Pará;

V – Ações destinadas a assegurar o funcionamento dos processos e a continuidade da prestação jurisdicional, além da continuidade operacional e administrativa do Poder Judiciário do Estado do Pará;

VI - Ações de planejamento, sistematização e normatização sobre temas atinentes à segurança cibernética;

VII - Ações de comunicação, conscientização, formação de cultura e direcionamento institucional, objetivando elevar a maturidade em segurança cibernética; e

VIII – Ações de qualificação específicas em segurança cibernética para os servidores lotados na Secretaria de Informática.

Art. 40. O cumprimento destas normas se dará através da atuação conjunta da Secretaria de Informática, do Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA) e da Escola Judicial do Poder Judiciário do Estado do Pará (EJPA), que deverão desenvolver ações de formação de competências, capacitação, reciclagem, conscientização e fomento em segurança cibernética, podendo incluir, entre outras iniciativas:

I – Inclusão de tópicos relativos à segurança da informação em cursos de formação inicial para magistrados e servidores que ingressarem no Poder Judiciário do Estado do Pará.

II - Ações periódicas de treinamento em nível de conhecimento básico, intermediário e avançado para os usuários dos recursos de TIC do Tribunal;

III – Programas de desenvolvimento de competências em segurança cibernética para servidores lotados na Secretaria de Informática;

IV – Programas de intercâmbio, imersão e cooperação com órgãos da Administração Pública, iniciativa privada e o meio acadêmico;

V – Palestras, congressos, seminários, workshops e afins;

VI – Programas de certificação especializada para analistas judiciários e auxiliares judiciários lotados na Secretaria de Informática e que estão envolvidos diretamente com o tema de segurança cibernética;

VII – Formação de nível acadêmico em segurança cibernética, visando a formação de especialistas.

Parágrafo Único As ações previstas deverão ser priorizadas no formato considerado mais efetivo em termos de adequação ao aprendizado, ao aproveitamento e aos objetivos pretendidos, podendo ser realizada, em âmbito nacional ou internacional, nas modalidades presencial, online ou híbrida.

Art. 41. O Poder Judiciário do Estado do Pará, através, da atuação conjunta da Secretaria de Informática, do Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA) e da Escola Judicial do Poder Judiciário do Estado do Pará (EJPA), também deve desenvolver ações de amplo alcance dos usuários, tais como:

I – Campanhas educativas e ações formativas;

II – Produção e divulgação de produtos de comunicação gráfica e digital nos canais oficiais do Tribunal de Justiça do Estado do Pará;

III – Testes públicos de segurança.

Art. 42. Caberá ao Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA) propor revisões e atualizações para estas normas, bem como metas a serem alcançadas por parte das ações desenvolvidas.

Art. 43. O Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA) poderá consultar a Escola Judicial do Poder Judiciário do Estado do Pará (EJPA) sobre os resultados das ações desenvolvidas e definir ações de incentivo para o cumprimento das metas que forem estabelecidas.

SEÇÃO IV

NORMAS DE GESTÃO DE ACESSOS PARA USUÁRIOS

Art. 44. Estas normas visam atender, no âmbito do Poder Judiciário do Estado do Pará, a necessidade de se estabelecer e gerenciar controles de acesso dos usuários aos recursos de TIC do Tribunal.

Art. 45. São objetivos das Normas de Gestão de Acesso para Usuários, não se limitando a estes:

I – Implantar, no âmbito do Poder Judiciário do Estado do Pará, uma estratégia de privilégio mínimo, visando evitar acessos indevidos e vazamento de dados;

II – Aprimorar a segregação de funções, estabelecendo papéis e responsabilidades na execução da gestão de acessos;

III – Conscientizar os usuários sobre a necessidade de ter acesso apenas às informações e aos recursos de TIC que sejam necessários para o cumprimento de suas atividades.

SUBSEÇÃO I

GERENCIAMENTO DE ACESSO LÓGICO

Art. 46. Preferencialmente, o controle de acesso deve ser baseado em papéis, utilizando o modelo *Role-based access control* (RBAC).

Art. 47. O acesso aos recursos de TIC do Tribunal será concedido apenas a usuários (as) autenticados (as) e autorizados (as) para uso desses recursos.

Parágrafo Único. Os responsáveis pelos recursos de TIC devem estabelecer regras de controle de acesso e papéis com permissões adequadas aos usuários (as) que realizarão os acessos.

Art. 48. Será estabelecido um processo formal, preferencialmente automatizado, para realizar a concessão e a revogação de acessos aos recursos de TIC, onde haverá responsáveis pelas etapas de solicitação, administração, concessão, bloqueio e revogação de acesso.

§ 1º Os responsáveis pelos recursos de TIC devem estabelecer regras de concessão, bloqueio e revogação de acesso ao recurso, levando em conta a Política de

Segurança da Informação do Poder Judiciário do Estado do Pará (PSI-PJPA) e suas normas.

§ 2º Os acessos aos recursos de TIC devem ser retirados imediatamente após o encerramento das atividades, em caso de mudança de papéis ou após a conclusão do processo de revogação do usuário do recurso de TIC ou incidente cibernético (de acordo com o item III, § 7ª do art. 52)

§ 3ª As contas utilizadas devem ser apenas desabilitadas, ao invés de serem excluídas, visando a preservação de dados para realização de auditorias, quando necessário.

Art. 49. A criação de nomes de usuário (a) e de contas de e-mail seguirá critérios definidos pela Secretaria de Informática.

Parágrafo Único. O nome de usuário (a) não poderá ser alterado, exceto quando houver alguma mudança em seu nome, onde o interessado (a) precisará manifestar a necessidade junto à Secretaria de Gestão de Pessoas e à Secretaria de Informática.

Art. 50. A Secretaria de Informática deve estabelecer e manter um inventário de todas as contas relacionadas abaixo, incluindo data de criação e de término da validade, quando for o caso:

I – Contas de usuário padrão, tanto de domínio, quanto local, incluindo o recurso de TIC no qual está presente a conta local;

II – Contas de administrador local, incluindo o recurso de TIC no qual está presente a referida conta;

III – Contas de administrador de domínio, incluindo os recursos de TIC nos quais o administrador pode acessar.

Parágrafo Único. A Secretaria de Informática deve avaliar semestralmente a necessidade de as contas permanecerem ativas e com os níveis de privilégio que possuem no momento da avaliação, podendo realizar as alterações necessárias para manter os níveis de segurança estabelecidos.

Art. 51. A Secretaria de Informática deve manter um inventário dos sistemas de autenticação existentes no Tribunal, tanto internamente, quanto hospedados externamente.

SUBSEÇÃO II

GESTÃO DE IDENTIDADES

Art. 52. A criação de acessos a recursos de TIC e de atribuições de papéis ou perfis de acesso a usuários, será solicitada pela chefia imediata do usuário e deve ser realizada através de chamado específico na Central de Serviços do Tribunal.

§ 1º A chefia imediata deve informar o perfil de acesso do usuário (a) à rede local ou ao sistema ou aplicação pretendida, sendo que este perfil deve ser restrito ao desempenho das atividades do usuário (a);

§ 2º O gestor do recurso de TIC será responsável pela autorização do acesso e poderá designar equipe técnica para operacionalizar o acesso;

§ 3º A autorização do acesso ao (a) usuário (a) não deve ser realizada enquanto não houver a autorização formal do gestor (a) do recurso de TIC;

§ 4º As autorizações concedidas devem ser documentadas, para fins de auditoria e análise periódica, visando detectar acessos indevidos;

§ 5º O (a) usuário (a) que será cadastrado deve ser identificado pela equipe responsável para, assim, ter seu cadastro confirmado;

§ 6º Caso haja mudança nas atribuições do (a) usuário (a), mudança de lotação ou qualquer outro motivo que leve à suspensão de suas atividades, o acesso do (a) usuário (a) deve ser direcionado para um perfil padrão e ser removido qualquer papel associado, até que a chefia solicite um novo perfil ou aconteça o retorno às atividades;

§ 7º Após o cadastro do (a) usuário (a), ele (a) deverá, através de um Termo de Responsabilidade de Acesso:

I – Declarar o conhecimento e aceitação dos termos da Política de Segurança da Informação do Poder Judiciário do Estado do Pará (PSI-PJPA) e de suas Normas, não podendo, a qualquer tempo, alegar desconhecimento ou ignorância destes termos;

II – Estar ciente que o acesso à rede de dados do Tribunal, bem como correio eletrônico, sistemas, aplicações internas e outros acessos correlatos são passíveis de auditoria;

III – Declarar que manterá a confidencialidade e segurança de sua credencial, entendendo que ela será alterada periodicamente em condições a serem definidas

pela Secretaria de Informática, inclusive podendo o acesso ser bloqueado, caso a Secretaria de Informática encontre indícios de comprometimento da credencial.

Art. 53. Compete ao (a) gestor (a) do recurso de TIC realizar a revisão dos níveis de privilégios concedidos aos (às) usuários (as) para o recurso sob sua responsabilidade, podendo a Secretaria de Informática, caso seja possível, automatizar o processo de mudança de privilégios e alterações de perfis e papéis dos (as) usuários (as).

Art. 54. A Secretaria de Informática deve manter o registro de todos os eventos significativos sobre o uso e a gestão de identidade dos (as) usuários (as), bem como informações de autenticação e acesso à rede, sistemas, aplicações e outros recursos que necessitam de identificação do (a) usuário (a).

Art. 55. Os (as) usuários (as) devem possuir identificação (*login*) única e exclusiva para fins de responsabilidade.

§ 1º Não deve ser realizado cadastro que gere identificação genérica ou ambígua do (a) usuário (a).

§ 2º Os acessos serão criados com o privilégio mínimo necessário para que os (as) usuários (as) dos recursos exerçam suas atividades institucionais.

Art. 56. Identidades compartilhadas entre vários usuários (as) só serão permitidas mediante autorização do Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA) e da Secretaria de Informática, além do compartilhamento de responsabilidades entre as chefias imediatas dos (as) usuários (as), pelo uso da identidade compartilhada.

Art. 57. Compete às chefias imediatas dos (as) usuários (as) dos recursos de TIC comunicar aos respectivos gestores (as) sobre a movimentação ou desligamento de usuários (as) de seu setor, para que sejam revistos os referidos acessos.

§ 1º A mudança nos acessos do (a) usuário (a) somente será efetuada após a confirmação da movimentação ou desligamento do (a) usuário (a) no sistema de recursos humanos utilizado no TJPA;

§ 2º A Secretaria de Informática realizará o bloqueio automático das credenciais do (a) usuário (a) que não realizar acessos por mais de 30 (trinta) dias;

§ 3º Caso a inatividade do acesso citado no parágrafo anterior tenha ocorrido por motivos legítimos, o (a) usuário (a) pode solicitar a reativação de seu acesso através da Central de Serviços do Tribunal.

Art. 58. Os níveis de privilégios concedidos aos (às) usuários (as) dos recursos de TIC devem ser revistos, no mínimo, trimestralmente, e em caso de suspeita de ataques cibernéticos, de forma imediata.

Art. 59. Identidades digitais utilizadas por serviços e sistemas de TIC, independente do ambiente em que estejam hospedados, também estão sujeitas a estas normas, onde:

I – A Secretaria de Informática deverá manter um inventário com as contas citadas no *caput* deste artigo, contendo, no mínimo, o sistema ou serviço onde a identidade está sendo utilizada, o propósito para sua utilização, o responsável pelo sistema ou serviço e a data de revisão do acesso;

II – Deverão ser adotados requisitos de tamanho, complexidade, periodicidade de rotação e expiração de credenciais que sejam compatíveis com estas normas;

III – Deverá ser realizada uma análise periódica, no mínimo semestralmente, sobre a necessidade de manter a autorização e o uso destas identidades;

IV – Deverão ser adotados mecanismos seguros para armazenamento e trânsito das credenciais utilizadas por estas identidades;

V – Deverão ser realizados o registro e o armazenamento de todos os eventos significativos envolvendo o uso destas identidades, com o objetivo de auxiliar no subsídio de informações para identificação de ataques cibernéticos.

Art. 60. Caso seja possível, devem ser inseridas cláusulas de sanções nos contratos sob gestão da Secretaria de Informática para tentativas de acesso ou acessos não autorizados por parte dos prestadores de serviço, incluindo colaboradores (as) diretos e indiretos.

SUBSEÇÃO III

SENHAS

Art. 61. Os recursos de TIC que serão objeto de controle de acesso por parte de seus respectivos gestores (as), terão seu acesso restrito através de métodos de autenticação que incluam a utilização de senhas, *tokens* ou outros aprovados pelo Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA) e pela Secretaria de Informática.

§ 1º O Acesso remoto, o acesso privilegiado e o acesso a recursos internos de TIC que estejam expostos diretamente na Internet serão realizados através de *Multifactor Authentication* (MFA);

§ 2º Caso a Secretaria de Informática, juntamente com o (a) gestor (a) do recurso, avalie um recurso de TIC como crítico, deverá implementar a utilização de *Multifactor Authentication* (MFA).

Art. 62. Caso necessário, serão concedidas credenciais com utilização de senha temporárias, mediante concordância e termo de confidencialidade, ou outro mecanismo de autenticação disponível e que seja autorizado pela Secretaria de Informática.

Parágrafo Único. O Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA) e a Secretaria de Informática deverão instituir processo de identificação do (a) solicitante, cabendo o tratamento dos dados pessoais fornecidos para a realização da identificação.

Art. 63. As senhas, *tokens* ou outros mecanismos de autenticação utilizados são de uso pessoal e intransferível, devendo o (a) usuário (a) zelar por sua guarda e sigilo.

§ 1º Será vedada a emissão de senhas, *tokens* ou outros mecanismos de autenticação para ciência de terceiros, ainda que chefes (as) imediatos ou superiores dos usuários (as);

§ 2º O (a) usuário (a) é responsável pela utilização de sua senha, token ou outro mecanismo de autenticação autorizado e sua utilização indevida poderá acarretar, de forma isolada ou cumulativamente, nos termos da legislação vigente, em sanções administrativas, civis e penais.

Art. 64. As senhas terão recomendações de complexidade e utilização regulamentadas em normativo próprio, a ser aprovado pelo Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA) e pela Secretaria de Informática.

Art. 65. A Secretaria de Informática deverá manter um sistema de gerenciamento de senhas que:

I – Permita a modificação da senha pelo (a) próprio (a) usuário (a), além da confirmação da modificação para evitar erros;

II – Permita a modificação da senha temporária no primeiro acesso ao respectivo recurso de TIC;

III – Recomende e oriente sobre o uso de senhas fortes;

IV – Mantenha um registro das senhas utilizadas anteriormente, não permitindo a reutilização delas;

V – Utilize criptografia no tráfego e no armazenamento das senhas;

VI – Garanta a mudança das senhas em intervalos regulares, a serem definidos pelo Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA) e pela Secretaria de Informática.

VII - Não exiba senhas digitadas nas telas;

VIII - Permita auditoria dos acessos e das operações realizadas com a senha;

IX - Monitorar trocas de senhas utilizadas em acessos privilegiados;

X - Monitorar tentativas de acesso a contas desativadas;

SUBSEÇÃO IV

ACESSO PRIVILEGIADO

Art. 66. O acesso privilegiado aos recursos de TIC do Tribunal apenas será concedido aos (às) servidores (as) lotados (as) na Secretaria de Informática que sejam gestores (as) desses recursos e que tenham a necessidade de administrá-los, ou a servidores (as) ou terceirizados (as) que realizem essa administração de forma delegada pelo gestor (a).

§ 1º Os (as) gestores (as) dos recursos de TIC e os (as) servidores (as) que realizem tarefas delegadas pelo (a) gestor (a) deverão estar capacitados e possuir as competências necessárias para realizar as tarefas que exijam acesso privilegiado;

§ 2º Usuários (as) diferentes dos citados no § 1º que solicitem acesso privilegiado a algum recurso de TIC deverão ser autorizados pelo Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA) e pela Secretaria de Informática;

§ 3º O acesso privilegiado deverá ser concedido através de contas com credenciais exclusivas para tal finalidade e distintas do utilizado para atividades cotidianas;

§ 4º A Secretaria de Informática deverá estabelecer um processo específico para autorizar e conceder acessos privilegiados, além de manter o registro desses pedidos para fins de auditoria e definir prazos de expiração do acesso concedido;

§ 5º Os requisitos para a realização de acessos privilegiados deverão ser mais complexos e incluir, no mínimo e não se limitando a estes:

I – Comprimento e complexidade de credenciais maiores do que em acessos não-privilegiados;

II – Tempo de rotação de credencial menor do que em acessos não-privilegiados;

III – Uso de MFA (*Multifactor Authentication*);

IV – Uso de soluções específicas para realização de acesso privilegiado, quando couber.

Art. 67. As tarefas realizadas que dependam de acesso privilegiado deverão ter sua necessidade avaliada de forma periódica, no mínimo trimestralmente, pela Secretaria de Informática.

Art. 68. Em caso de necessidade de acesso privilegiado por parte de fornecedores (as) com os quais o Tribunal possua contrato, para a realização de tarefas aprovadas pela Secretaria de Informática, o acesso será temporário e apenas pelo tempo necessário para a realização das tarefas.

Art. 69. O acesso privilegiado realizado através de *contas* administrativas genéricas ou que sejam padrões dos recursos de TIC do Tribunal deverá ser evitado sempre que possível.

§ 1º Caso somente seja possível realizar o acesso privilegiado com uma conta administrativa genérica ou padrão da solução, a Secretaria de Informática deverá, se possível, habilitar o uso de MFA (*Multifactor Authentication*), realizar rotação periódica da credencial e auditar os acessos realizados;

§ 2º Sendo possível, a conta administrativa genérica deverá ser renomeada, com o objetivo de dificultar sua identificação;

§ 3º Em caso de mudança do (a) gestor (a) do recurso de TIC, do (a) servidor (a) ou do (a) terceirizado (a) que realize tarefas delegadas pelo (a) gestor (a), a credencial da conta administrativa genérica ou padrão da solução deve ser alterada imediatamente.

SUBSEÇÃO V

ACESSO REMOTO AOS RECURSOS DE TIC DO TRIBUNAL

Art. 70. Os (as) usuários (as) que estiverem em teletrabalho ou que forem autorizados (as) por suas chefias imediatas, mediante justificativa, poderão solicitar acesso remoto aos recursos de TIC do Tribunal através da abertura de chamado na Central de Serviços do Tribunal.

§ 1º Entende-se por acesso remoto o acesso disponibilizado pela Secretaria de Informática, através de VPN (*Virtual Private Network*), Portal de Aplicações ou outro meio que a Secretaria de Informática entender que tenha nível de segurança adequado, a recursos de TIC internos através de meio de conectividade externo (Internet), de acordo com as características de cada recurso a ser acessado;

§ 2º A chefia imediata deverá especificar no chamado aberto quais são os recursos que o (a) usuário (a) poderá acessar quando utilizar o acesso remoto, observando o princípio do privilégio mínimo;

§ 3º Após a liberação do acesso, o (a) usuário (a) deverá, através de um Termo de Responsabilidade referente ao acesso remoto:

I – Declarar o conhecimento e aceitação dos termos da Política de Segurança da Informação do Poder Judiciário do Estado do Pará (PSI-PJPA) e de suas Normas, não podendo, a qualquer tempo, alegar desconhecimento ou ignorância destes termos;

II – Estar ciente que a utilização do acesso remoto será passível de auditoria;

III – Declarar que manterá a confidencialidade e segurança de sua credencial utilizada para realizar o acesso remoto, entendendo que ela será alterada periodicamente em condições a serem definidas pela Secretaria de Informática, inclusive podendo o acesso ser bloqueado, caso a Secretaria de Informática encontre indícios de comprometimento da credencial.

Art. 71. Acessos remotos que tenham origem de fora do Brasil devem ser autorizados pelo Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA) e pela Secretaria de Informática.

Art. 72. Será obrigatório a utilização de MFA (*Multifactor Authentication*) ao realizar o *login* inicial para uso do acesso remoto.

Art. 73. O acesso remoto aos recursos de TIC do Tribunal não poderá ser realizado a partir de computadores públicos e redes sem fio públicas.

Art. 74. O suporte técnico para o acesso remoto estará disponível durante o horário de expediente do Tribunal.

Art. 75. Os eventos referentes ao uso do acesso remoto, devem ser armazenados por um período mínimo de 1 (um) ano, com a finalidade de identificar acessos indevidos.

SEÇÃO V

NORMAS PARA GESTÃO DE VULNERABILIDADES

Art. 76. Estas normas visam atender, no âmbito do Poder Judiciário do Estado do Pará, a necessidade de controles mínimos sugeridos pelo Manual de Proteção de Infraestruturas Críticas de TIC, estabelecido pela Portaria nº 162/2021, do Conselho Nacional de Justiça-CNJ, para gerenciamento contínuo de vulnerabilidades.

Art. 77. São objetivos das Normas para Gestão de Vulnerabilidades do Poder Judiciário do Estado do Pará (PGV-PJPA), não se limitando a estes:

I – Analisar proativamente o parque computacional do Poder Judiciário do Estado do Pará, visando a identificação de vulnerabilidades que possam ser exploradas em ataques cibernéticos;

II – Analisar informações fornecidas pelos fabricantes das soluções de TIC do Poder Judiciário do Estado do Pará, com o objetivo de priorizar e corrigir as vulnerabilidades identificadas;

III – Classificar o risco das vulnerabilidades identificadas, com o objetivo de determinar o tempo máximo de correção dessas vulnerabilidades;

IV – Contribuir na promoção da resiliência cibernética no âmbito do Poder Judiciário do Estado do Pará.

V – Contribuir na construção de um processo automatizado de análise, avaliação, registro e correção de vulnerabilidades que seja conhecido e cumprido no âmbito da Secretaria de Informática.

Art. 78. A Secretaria de Informática deve manter um inventário completo e atualizado das soluções de TIC utilizadas, com seu respectivo responsável e nível de criticidade para o Poder Judiciário, permitindo a aplicação desta política de forma mais efetiva.

Art. 79. A Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) do Poder Judiciário do Estado do Pará, juntamente com a Secretaria de Informática devem, proativamente e periodicamente, obter informações sobre possíveis vulnerabilidades existentes no parque computacional do Poder Judiciário do Estado do Pará, através de consultas em fontes confiáveis, como as relacionadas abaixo:

I – Boletins de segurança dos fabricantes das soluções de TI utilizadas no Poder Judiciário do Estado do Pará;

II – Boletins de segurança de equipes de tratamento e resposta a incidentes (ETIR) de outros órgãos da Administração Pública Federal, Estadual e Municipal;

III – Comunidades especificamente criadas para troca de alertas de segurança cibernética entre os integrantes;

IV – *Sites* especializados em segurança da informação e segurança cibernética.

Art. 80. Para contribuir na obtenção de informações sobre vulnerabilidades, serão realizados, através de solução tecnológica própria para este fim, verificações periódicas (varreduras ou *scans*) em todo o parque computacional do Poder Judiciário do Estado do Pará, que terão como objetivo encontrar:

I – Vulnerabilidades em ativos expostos à Internet;

II – Vulnerabilidades em ativos considerados críticos para o Poder Judiciário do Estado do Pará;

III – Vulnerabilidades consideradas como de fácil exploração;

IV – Vulnerabilidades avaliadas por ferramentas especializadas como de nível crítico;

V – Vulnerabilidades avaliadas por ferramentas especializadas como de nível alto;

VI – Vulnerabilidades avaliadas por ferramentas especializadas como de nível médio.

§ 1º A periodicidade dos *scans* a serem realizados será definida pela Secretaria de Informática, sendo obrigatório realizar, no mínimo, 1 (um) *scan* autenticado e 1 (um) *scan* não-autenticado por mês, de forma automatizada.

§ 2º Para realizar o *scan* autenticado, a Secretaria de Informática deve disponibilizar uma conta específica com permissão de *login* nos ativos a serem avaliados e com nível de privilégio que permita a análise mais completa que seja possível realizar nos ativos.

§ 3ª Os resultados dos *scans* devem ser comparados, para se seja possível verificar o comportamento do quadro de vulnerabilidades ao longo do tempo.

Art. 81. Os usuários de TIC do Poder Judiciário do Estado do Pará que tiverem conhecimento ou suspeita de vulnerabilidades em ativos sob sua responsabilidade, devem notificá-las para a ETIR do Tribunal, de forma mais breve possível, sem a necessidade de autorização da chefia imediata.

Parágrafo Único. A notificação pode ser realizada através de abertura de chamado na Central de Serviços, por e-mail para os endereços etir@tjpa.jus.br e seginfo@tjpa.jus.br, ou diretamente na Secretaria de Informática.

Art. 82. Caso sejam encontradas vulnerabilidades em algum ativo, elas não devem ser objeto de teste por parte dos usuários de TIC e dos integrantes da SECINFO, sob risco de danos ao ativo e comprometimento da prestação jurisdicional.

Art. 83. A Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) do Poder Judiciário do Estado do Pará deve dar amplo conhecimento das vulnerabilidades identificadas para:

I – O responsável pelo ativo vulnerável;

II – O chefe do Serviço, Divisão ou Coordenadoria responsável pelo ativo vulnerável;

III – O Secretário de Informática;

IV – O Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA).

Art. 84. A Secretaria de Informática deve criar um repositório centralizado, onde as vulnerabilidades encontradas devem ser registradas e categorizadas, contendo, no mínimo, as seguintes informações:

I – Código CVE (*Common Vulnerabilities and Exposures*) para identificação da vulnerabilidade encontrada;

II – CVSS (*Common Vulnerabilitiy Score System*) para avaliação da gravidade da vulnerabilidade;

III – Ativo vulnerável e seu responsável;

IV – Ação a ser tomada para correção da vulnerabilidade;

V – Tempo estimado para correção da vulnerabilidade.

Art. 85. A Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) do Poder Judiciário do Estado do Pará, com a colaboração da Secretaria de Informática, fica responsável por elaborar um processo de gestão de vulnerabilidades para o cumprimento desta Política.

SEÇÃO VI

NORMAS DE SEGURANÇA PARA TELETRABALHO

Art. 86. Estas normas visam atender a necessidade de se estabelecer controles de segurança específicos para os usuários dos recursos de TIC, que exercem suas atividades na modalidade Teletrabalho.

Art. 87. O usuário que aderir ao regime de Teletrabalho do Tribunal deve, obrigatoriamente, utilizar um notebook corporativo, entregue pela Secretaria de Informática que contenha, no mínimo, as seguintes proteções:

I - Proteção contra *malwares;*

II - Proteção para credenciais de acesso local;

III – Software para distribuição de correções de vulnerabilidades de sistema operacional;

IV – Software para monitoramento contra perda ou furto do equipamento;

V – Software para auditoria e conformidade em segurança cibernética;

VI – *Firewall* pessoal.

§ 1º Havendo motivo justificado e sendo autorizado pela Secretaria de Informática, em conjunto com o Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA), o (a) usuário (a) poderá utilizar um *notebook* pessoal para desempenhar suas atividades em Teletrabalho.

§ 2º O *notebook* pessoal do (a) usuário (a) que for autorizado passará por avaliação técnica da Secretaria de Informática, no que diz respeito às proteções de segurança definidas no *caput* deste artigo.

§ 3º Caso não se observe uma ou mais proteções de segurança no *notebook* pessoal do (a) usuário (a), a Secretaria de Informática não autorizará este dispositivo para uso no ambiente de Teletrabalho do Tribunal.

§ 4º Os (as) usuários (as) que não tiverem seus *notebooks* pessoais autorizados para uso no Teletrabalho do Tribunal terão até 90 (noventa) dias para agendar e receber notebooks corporativos por parte da Secretaria de Informática, sob pena de serem suspensos do regime de Teletrabalho.

§ 5º A Secretaria de Informática não prestará suporte técnico para problemas de *hardware* ou *software* do *notebook* pessoal do (a) usuário (a).

Art. 88. O *notebook* corporativo deve ser utilizado exclusivamente pelo (a) usuário (a) ao qual foi concedido o uso, não podendo este notebook ser compartilhado com outras pessoas do Tribunal ou fora dele.

Art. 89. O (a) usuário (a) só terá autorização de acesso aos sistemas e aplicações que sejam pertinentes com suas atividades.

Parágrafo Único. O acesso a sistemas e aplicações internas do Tribunal deve ser realizado através de acesso remoto concedido pelo Tribunal, de acordo com as normas elencadas na Seção V (Normas de Gestão de Acessos para Usuários), Subseção IV (Acesso Remoto aos Recursos de TIC do Tribunal) da Política de Segurança da Informação do Poder Judiciário do Estado do Pará (PSI-PJPA), ou por outro método de acesso seguro que o Tribunal disponibilizar.

Art. 90. Os dados armazenados no notebook corporativo devem ser pertinentes as atividades desenvolvidas pelo (a) usuário (a), que também deve ter a responsabilidade de copiar estes dados para o serviço de nuvem oferecido pelo Tribunal, visando a proteção destes dados em caso de dano, perda ou furto do equipamento.

Parágrafo Único. A Secretaria de Informática não se responsabilizará por dados particulares do (a) usuário (a) que tiverem sido armazenados no notebook corporativo e que tenham sido perdidos por motivo de dano, perda ou furto do equipamento.

Art. 91. Os notebooks corporativos utilizados no ambiente de Teletrabalho serão objeto de auditorias regulares por parte da Secretaria de Informática, com o objetivo de manter a conformidade do equipamento com estas normas e com a Política de Segurança da Informação do Poder Judiciário do Estado do Pará (PSI-PJPA).

Art. 92. Os (as) usuários (as) em Teletrabalho devem utilizar, para fins de autenticação, a tecnologia MFA (*Multifactor Authentication*) em todos os aplicativos e sistemas que o Tribunal utiliza e que são compatíveis com a tecnologia.

Art. 93. É vedada a utilização de soluções de acesso remoto de terceiros, sem a autorização expressa da Secretaria de Informática.

Parágrafo Único. Sendo autorizada a utilização de uma solução de acesso remota, deve-se optar por soluções corporativas que, preferencialmente, possuam um fator duplo de autenticação habilitado.

Art. 94. Em caso de dano, perda ou furto do notebook corporativo, o (a) usuário (a) deve avisar imediatamente a Secretaria de Informática para que sejam tomadas as providências cabíveis.

SEÇÃO VII

NORMAS PARA USO DE DISPOSITIVOS MÓVEIS

Art. 95. Estas normas visam definir diretrizes para a utilização segura de dispositivos móveis, no âmbito do Poder Judiciário do Estado do Pará, visando a mitigação de riscos cibernéticos e a proteção de dados institucionais armazenados nestes dispositivos, aumentando a maturidade em segurança cibernética do Tribunal.

Art. 96. Os dispositivos móveis corporativos devem ser inventariados e possuir um responsável designado para responder pelo dispositivo.

Art. 97. Apenas será autorizado a utilizar o dispositivo o (a) magistrado (a) ou servidor (a) cadastrado (a) como responsável pelo mesmo e que tenha consciência das normas contidas na Política de Segurança da Informação do Poder Judiciário do Estado do Pará (PSI-PJPA).

Art. 98. Devem ser instalados nos dispositivos móveis corporativos apenas aplicativos homologados pela Secretaria de Informática.

Parágrafo único. Caso seja necessária a utilização de algum aplicativo que não seja homologado, ele passará por avaliação pela SECINFO, podendo ser permitida ou negada sua instalação.

Art. 99. Os dispositivos móveis corporativos devem ser autenticados na rede de dados do Tribunal, onde o dispositivo e sua conectividade serão monitorados, a fim de garantir o controle de acesso necessário e a compatibilidade com a Política de Segurança da Informação do Poder Judiciário do Estado do Pará (PSI-PJPA).

Art. 100. Os dispositivos móveis corporativos devem possuir mecanismos de proteção e sigilo dos dados institucionais armazenados, com o objetivo de prevenir o roubo ou o vazamento destes dados em casos de ataques cibernéticos, ou mesmo de furto ou extravio do dispositivo.

Art. 101. Os dispositivos móveis corporativos poderão passar por análise de vulnerabilidades e, caso seja detectada alguma vulnerabilidade de nível crítico, alto ou médio, o dispositivo deve ser encaminhado para a Secretaria de Informática para que se efetuem as devidas correções. Caso o dispositivo móvel não esteja em conformidade com a Política de Segurança da Informação do Poder Judiciário do Estado do Pará (PSI-PJPA), não poderá ser utilizado na rede de dados do Tribunal.

Art. 102. Só poderá utilizar o dispositivo móvel particular o (a) magistrado (a) ou servidor (a) que tenha sido autorizado pela Secretaria de Informática e que tenha consciência das normas contidas na Política de Segurança da Informação do Poder Judiciário do Estado do Pará (PSI-PJPA).

Art. 103. Os dispositivos móveis particulares devem ser autenticados na rede de dados do Tribunal, onde o dispositivo e sua conectividade serão monitorados, a fim de garantir o controle de acesso necessário e a compatibilidade com a Política de Segurança da Informação do Poder Judiciário do Estado do Pará (PSI-PJPA).

Parágrafo Único A Secretaria de Informática será responsável por autorizar o acesso aos recursos de TIC do Tribunal através de dispositivos móveis particulares.

Art. 104. Os dispositivos móveis particulares devem possuir mecanismos de proteção e sigilo dos dados institucionais armazenados, providenciados por seus respectivos usuários, com o objetivo de prevenir o roubo ou o vazamento destes dados em casos de ataques cibernéticos, ou mesmo de furto ou extravio do dispositivo.

Art. 105. Os dispositivos móveis particulares poderão passar por análise de vulnerabilidades e, caso sejam detectadas vulnerabilidades de nível crítico, alto ou médio, o usuário será alertado pela Secretaria de Informática para que sejam efetuadas as devidas correções.

Parágrafo único Caso as correções informadas pela Secretaria de Informática não sejam efetuadas, o (a) usuário (a) não poderá mais utilizar o referido dispositivo na rede de dados do Tribunal e os dados institucionais que estiverem armazenados devem ser retirados do dispositivo.

Art. 106. A Secretaria de Informática será responsável por realizar o controle de acesso e autorizar apenas o acesso à internet para dispositivos móveis visitantes, através de uma rede de dados totalmente isolada.

SEÇÃO VIII

NORMAS PARA BACKUP E RESTAURAÇÃO DE DADOS

Art. 107. Estas normas visam definir, no âmbito do Poder Judiciário do Estado do Pará, responsabilidades e competências para a proteção e a disponibilidade dos dados custodiados pelos administradores das soluções utilizadas no Tribunal, visando a continuidade da prestação jurisdicional dos serviços para a sociedade paraense.

Art. 108. Todos os serviços que forem avaliados como críticos pela Secretaria de Informática serão alvo das Normas para Backup e Restauração de Dados.

§ 1º Também serão alvo destas normas os dados contidos em:

I – Servidores de arquivos;

II – Servidores de aplicações;

III – Servidores de banco de dados;

IV – Servidores de e-mail e mensageria;

V – Máquinas virtuais com serviços diversos aos relatados nos itens anteriores;

VI – Demais serviços críticos, definidos de acordo com o Art. 4º desta política.

§ 2º A recuperação de serviços hospedados localmente na infraestrutura computacional do tribunal deve abranger os dados e os componentes necessários para o retorno de seu pleno funcionamento.

§ 3º Dados que estejam armazenados apenas localmente nas estações de trabalho que compõem o parque computacional do TJPA não serão objeto destas normas, sendo responsabilidade dos (as) usuários (as) manter os dados salvos e protegidos.

I – Os (as) usuários (as) devem utilizar, preferencialmente, os serviços de armazenamento em nuvem disponibilizados pelo TJPA;

II – Em caso de descarte da estação de trabalho, a Secretaria de Informática deve assegurar que os dados contidos sejam apagados, de forma a se tornarem completamente irrecuperáveis;

III – Os dados contidos no backup apenas serão disponibilizados a usuários ativos do Tribunal, no pleno exercício de suas atribuições.

§ 4º A inclusão de novos serviços, críticos ou não, a terem seus dados protegidos, deve ser avaliada e sancionada pela Secretaria de Informática e pelo comitê de Governança de Segurança da Informação (CGSI-PJPA).

Art. 109. A Secretaria de Informática será responsável por efetuar os processos de *backup*, validação e restauração dos dados tidos como escopo desta política.

Art. 110. Os dados e serviços incluídos originalmente como escopo destas normas e aqueles que forem solicitados posteriormente pelos respectivos responsáveis, quando solicitado, devem ser restaurados no menor tempo possível, visando prevenir a indisponibilidade de serviços críticos.

Art. 111. Caso haja falha total ou parcial no processo de cópia dos dados, o responsável pelo dado afetado deve ser notificado e, caso este julgue necessário, pode solicitar uma nova cópia.

Art. 112. No caso de perdas anteriores à execução do processo de cópia dos dados, não será possível realizar a recuperação desses dados.

Art. 113. Os dados copiados podem ser armazenados nos locais abaixo, não se limitando a estes:

I – Discos;

II – Fitas magnéticas;

III – Nuvem.

Art. 114. Os dados devem ser periodicamente copiados para um dispositivo de disco distinto daquele no qual se encontram, de tal forma que possam ser recuperados e restaurados, em caso de indisponibilidade ou perda dos dados de produção.

Art. 115. De acordo com a criticidade dos dados copiados, as cópias de segurança armazenadas primariamente em disco também podem ser armazenadas de forma secundária em fitas magnéticas ou em um ambiente de nuvem dedicado especificamente para este fim.

Art. 116. As mídias físicas utilizadas para *backup* devem ser guardadas em ambientes adequados, com controle de temperatura, umidade e outros fatores ambientais que possam ser considerados pela Secretaria de Informática como importantes para a conservação das mídias.

Art. 117. Os backups realizados devem ser testados de forma amostral, no mínimo uma vez por trimestre, de forma a assegurar a confiabilidade das mídias físicas e da nuvem utilizadas para o referido fim, além de comprovar a correta restauração dos dados.

Art. 118. As mídias que forem tidas como inservíveis ou inutilizadas devem ser descartadas de forma que impeça qualquer possibilidade de recuperação de dados por pessoas não autorizadas.

Art. 119. Os dados e serviços de TI do Poder Judiciário do Estado do Pará devem ser copiados, de forma padrão, de acordo com as frequências descritas abaixo:

I – Diária;

II – Semanal;

III – Mensal;

IV – Anual.

Art. 120. Os dados e serviços de TI do Poder Judiciário do Estado do Pará copiados de acordo com as frequências descritas no artigo anterior, terão, por padrão, os períodos de retenção relacionados a seguir:

I – *Backup* diário será retida pelo período de 1 (um) mês;

II – *Backup* semanal será retida pelo período de 6 (seis) meses;

III – *Backup* mensal será retida pelo período de 1 (um) ano;

IV – *Backup* anual será retida pelo período de 5 (cinco) anos.

Parágrafo Único. Caso o responsável pelos dados ou pelo serviço a ser copiado indique um tempo de retenção diferente dos períodos indicados neste artigo, o mesmo deve justificar a necessidade no momento de abertura do chamado técnico.

Art. 121. Sob acompanhamento e supervisão da Secretaria de Informática, devem ser realizados, no mínimo trimestralmente, testes de restauração completa do ambiente computacional do Poder Judiciário do Estado do Pará, com o objetivo de garantir a continuidade da prestação jurisdicional em caso de ataques cibernéticos que possam comprometer a infraestrutura de TI do Tribunal.

Art. 122. A cada teste realizado, deverá ser elaborado um relatório dos resultados alcançados e encaminhado para a Secretaria de Informática e para o Comitê de Governança de Segurança (CGSI-PJPA).

CAPÍTULO IV

REVISÃO E ATUALIZAÇÃO DA PSI-PJPA

Art. 123. O cumprimento, a conformidade e a melhoria contínua desta Política devem ser assegurados através de auditorias periódicas, tanto de cunho interno quanto externo, a serem realizadas em período não superior a 3 (três) anos. Os resultados das auditorias realizadas devem ser encaminhados para o Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA), que dará as tratativas para cumprimento das orientações indicadas nos relatórios e atualização da Política de Segurança da Informação do Poder Judiciário do Estado do Pará (PSI-PJPA) e das políticas, processos e procedimentos relacionados.

Art. 124. Caso haja motivos relevantes que tenham sido avaliados e ratificados pela Secretaria de Informática ou pelo Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA), a Política de Segurança da Informação do Poder Judiciário do Estado do Pará (PSI-PJPA) e as políticas, processos e procedimentos relacionados, podem ser revisados e atualizados imediatamente.

CAPÍTULO V

COMPETÊNCIAS E RESPONSABILIDADES

Art. 125. Esta Política deve ser amplamente divulgada, de forma permanente, através de ações de conscientização, a serem definidas pelo Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA), pela Secretaria de Informática, pela Escola Judicial do Poder Judiciário do Estado do Pará (EJPA) e pelo Departamento de Comunicação do Tribunal.

Parágrafo Único As chefias imediatas devem monitorar o cumprimento desta Política no âmbito de suas unidades, identificando possíveis dificuldades dos usuários e buscando meios para saná-las.

Art. 126. Todos os usuários que desempenham atividades no Poder Judiciário do Estado do Pará, tanto internamente como externamente, são responsáveis pela segurança da informação em todo o âmbito do PJPA e devem observar esta Política, zelando pela segurança dos recursos de TIC sob sua responsabilidade e pelos atos executados com suas respectivas credenciais de acesso.

Parágrafo Único O descumprimento desta Política poderá acarretar, de forma isolada ou cumulativamente, nos termos da legislação vigente, em sanções administrativas, civis e penais.

Art. 127. Compete à Presidência do Poder Judiciário do Estado do Pará, em conjunto com o Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA) determinar o direcionamento estratégico e fornecer os recursos necessários, visando garantir a estrutura adequada ao Sistema de Gestão de Segurança da Informação.

Art. 128. Os recursos orçamentários necessários para as ações de segurança da informação devem ser discriminados em rubrica específica para possibilitar que a Governança Nacional em Segurança Cibernética possa avaliar, de forma clara, os investimentos no setor.

Art. 129. O Poder Judiciário do Estado do Pará deve prover, além de recursos financeiros, recursos humanos e tecnológicos para o cumprimento desta Política, juntamente com suas normas.

Art. 130. Compete ao Gestor de Segurança da Informação coordenar ações referentes ao Sistema de Gestão de Segurança da Informação (SGSI), informando os resultados para a Secretaria de Informática, o Comitê de Governança de Segurança da

Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA) e a Presidência do Poder Judiciário do Estado do Pará.

Art. 131. A Secretaria de Informática será responsável pelo acompanhamento do uso dos ativos de TIC no âmbito do Tribunal e pelo cumprimento das normas referentes a estes.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 132. Os casos omissos serão levados para conhecimento e deliberação por parte do Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Pará (CGSI-PJPA), seguindo os objetivos, princípios e diretrizes estabelecidos nesta Portaria.

Art. 133. Esta Portaria entrará em vigor na data de sua publicação, revogando as Portarias 990/2009, 1045/2010, 1046/2010, 5745/2019 e 904/2022.

Publique-se. Registre-se. Cumpra-se

Belém, 30 de setembro de 2024

Maria de Nazaré Silva Gouveia dos Santos
Desembargadora Presidente do TJPA