ATA-GJAFSRJ - 22023
Código de validação: 65A381CC90

ATA DE REUNIÃO
COMITÊ DE GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO (CGSI) E COMITÊ GESTOR DE PROTEÇÃO DE DADOS (CGPD)

Ata da 5ª Reunião de 2023 (25/07/2023)

Aos vinte e cinco dias do mês de julho do ano de dois mil e vinte e três, na sala de videoconferência da DIA, utilizando a ferramenta ZOOM, às 09:00 horas, sob a coordenação do magistrado Francisco Soares Reis Júnior, designado pelo desembargador Jamil de Miranda Gedeon Neto, reuniram-se os membros do Comitês de Governança de Segurança da Informação (CGSI) e do Comitê Gestor de Proteção de Dados (CGPD), instituídos respectivamente pelas Resoluções RESOL-GP - 1132022 e RESOL-GP - 132021.

Como membros(as), registraram-se as presenças do juiz FRANCISCO SOARES REIS JÚNIOR (TJMA - Coordenador do CGPD e membro do CGSI), do juiz JOSÉ JORGE FIGUEIREDO DOS ANJOS JÚNIOR (CGJ - Membro do CGSI e CGPD), do juiz JOSÉ NILO RIBEIRO FILHO (TJMA - Coordenador do CGSI e membro do CGPD), do diretor CARLOS ANDERSON DOS SANTOS FERREIRA (Diretoria Geral - Membro do CGSI), do diretor CLÁUDIO HENRIQUE CARNEIRO SAMPAIO (Diretoria de Informática e Automação - Membro do CGSI e CGPD), do diretor LAÉRCIO LEÃO AMARAL (Diretoria Judiciária - Membro do CGPD), da diretora JUREMA MAMEDE DE PAIVA SANTOS (Diretoria de Auditoria Interna - Membra do CGPD), da diretora MILENA VIEIRA DE OLIVEIRA (Diretoria de Recursos Humanos - Membra do CGSI e CGPD), do diretor ANDRÉ MENEZES MENDES (Diretoria do FERJ - Membro do CGPD) e da assessora ISABELLA CAROLINA SILVA E SILVA (Assessoria de Comunicação da Presidência - Membra do CGSI).

Estavam ausentes os(as) membros(as): o desembargador JAMIL DE MIRANDA GEDEON NETO (TJMA - presidente do CGSI e CGPD), o diretor ALEXANDRE MAGNO DE SOUSA NUNES (Diretoria de Segurança Institucional e Gabinete Militar - Membro do CGSI e CGPD), a diretora CÉLIA REGINA PEREIRA DA SILVA (Diretoria Financeira - Membra do CGPD), substituída por FERNANDO ANTÔNIO CARVALHO MARQUES, a diretora KEILA FONSECA DA SILVA (Diretoria Administrativa - Membra do CGSI e CGPD), substituída por LUIZ GUSTAVO SANTOS NASCIMENTO, e o diretor MAYCO MURILO PINHEIRO (Diretoria de Engenharia - Membro do CGPD).

Como convidados, registraram-se as presenças de GIVANILDO MARQUES (Coordenadoria de Atendimento ao Usuário), MARCOS NAVA (Divisão de Serviços de

TI), PAULA GARDÊNIA COSTA SERRA (Gabinete da 2ª Vice-Presidência), CRISTIA LUCEIRO (INTEROP), HALLYSON CARLOS (INTEROP), FREDERICO COELHO e THIAGO VIEIRA (FAC Tecnologia).

A apresentação foi conduzida pelo diretor CLÁUDIO HENRIQUE CARNEIRO SAMPAIO com participação do Técnico Judiciário JAIRO FERREIRA ROCHA, servidor da Diretoria de Informática e Automação. A reunião foi iniciada com a pauta abaixo:

- Ações da ENSEC-PJ - Relatório de progresso;
- Normas da PSI (ANEXOS) - minutas para aprovação:

a. ANEXO VIII - Norma de Cópias de Segurança da Informação;
b. ANEXO IX - Norma de Gestão de Criptografia e Gerenciamento de Chaves;
c. ANEXO XII - Norma de Desenvolvimento Seguro;
d. ANEXO XVII - Norma de Gestão de Serviços em Nuvem.

- Ações da LGPD - Relatório de progresso;
- Ações futuras.

O Sr. Cláudio iniciou a reunião e passou a palavra para o Sr. Jairo Rocha que saudou a todos(as) e apresentou o relatório de progresso da ENSEC-PJ demonstrando sua evolução durante as reuniões dos Comitês. O progresso, focado na conclusão, evoluiu de 10,6% (31.01.2023) para 26,6% (20.03.2023), seguiu para 36,2% (09.06.2023) e atualmente está em 48,9% (24.07.2023).

Apresentou-se os processos do DIGIDOC nº 33841/2023 - Contratação de empresa especializada, para o fornecimento de Security Operations Center (SOC) e nº 33826/2023 - Contratação de treinamento e conscientização em Segurança da Informação dos(as) usuários(as) do PJMA.

Pontuou-se sobre a plataforma de treinamento e conscientização em cibersegurança da empresa HSC BRASIL. Solicitou-se a indicação de 02 (dois) nomes ao Sr. Laércio Leão e 02 (dois) nomes à Sra. Jurema Mamede para compor as vagas para validar o ambiente de testes **(demonstração)**. Ficou-se de verificar junto da empresa a possibilidade de 01 (uma) vaga para a Corregedoria Geral da Justiça, a pedido do MM. José Jorge.

Falou-se resumidamente sobre as normas de cópias de segurança da informação, de gestão de criptografia e gerenciamento de chaves, de desenvolvimento seguro e de gestão de serviços em nuvem, anexas a esta ata. O Sr. Cláudio Sampaio discorreu algumas palavras sobre dados, datacenter, backup e da importância dessas normas, com ênfase na norma de cópias de segurança da informação. Posteriormente,

as mesmas foram colocadas em votação pelos membros dos comitês e foram aprovadas por unanimidade.

Explanou-se sobre o andamento dos outros 04 (quatro) normativos: norma de gestão de incidentes de segurança da informação, norma de proteção de dados pessoais, norma de gestão de riscos de segurança da informação e o plano de gestão de continuidade de negócios.

Foi passada a palavra para o Sr. Frederico, da empresa FAC Tecnologia, que discorreu sobre o andamento das ações da LGPD de forma sucinta, conforme detalhamento abaixo:

- Workshop de mapeamento de dados pessoais para RH;
- Reuniões semanais com equipe do projeto e áreas envolvidas no mapeamento;
- Preenchimento das planilhas – TJMA, tira dúvidas e ajustes;
- Mapeamento:

a. **Finalizado:** Divisão de Cadastro e Coordenadoria de Direitos e Deveres;
b. **Em andamento:** Divisão de Expedição de Atos e Controles, Divisão de Seleção e Divisão de Avaliação e Desempenho;

- Envio de sugestão da Política de Privacidade - Minuta de Resolução;
- Envio de sugestão de melhorias no fluxo de atendimento aos titulares;
- Análise e sugestões de melhoria referente à Norma de Proteção de Dados Pessoais (PSI);
- Reunião com equipe do projeto, para apresentar nova estratégia de mapeamento de dados.
- Finalização dos mapeamentos do RH completo;
- Apresentação do mapeamento e riscos encontrados;
- Continuidade dos mapeamentos, priorizando área administrativa.

Por fim, o Sr. Cláudio Sampaio fez as considerações finais e franqueou espaço para os demais membros se manifestarem, onde o Sr. André Mendes parabenizou o Grupo de Trabalho Técnico em Segurança da Informação (GTT-SI) sobre a evolução das pautas dos comitês. A Sra. Paula, falando em nome do MM. Francisco Reis, que precisou se ausentar no final da reunião devido a uma audiência, trouxe algumas considerações da norma de desenvolvimento seguro para tratamento, e seguirá para publicação junto com as demais normas após saneamento e aval do magistrado. Não tendo mais assuntos a serem tratados a reunião foi encerrada, tendo eu, Cláudio Henrique Carneiro Sampaio, designado secretário ad hoc do Comitê, lavrado a presente ata que, depois de lida e aprovada, vai assinada pelos(as) membros(as) dos comitês.

PALÁCIO DA JUSTIÇA "CLÓVIS BEVILÁCQUA" DO ESTADO DO MARANHÃO

São Luís, 25 de julho de 2023.

ANEXO VIII

NORMA DE CÓPIAS DE SEGURANÇA DA INFORMAÇÃO

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo
Resolução nº 31/2015-GP	

Versionamento:

Versão:	1.0
Data:	02/05/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	24/07/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

1. INTRODUÇÃO

A norma de cópias de segurança da informação complementa a Política de Segurança da Informação (PSI), definindo as diretrizes de gestão das cópias de segurança produzidas pelo Poder Judiciário do Estado do Maranhão (PJMA).

Para fins desta norma, aplica-se a lista de termos do glossário com suas respectivas definições, conforme descrito no ANEXO I da PSI.

Esta norma obedece ao escopo definido na Política de Segurança da Informação, aplicando-se a todos os dados produzidos internamente e externamente no contexto do PJMA, incluindo dados armazenados em serviços de nuvem pública ou privada.

2. OBJETIVOS

Providenciar a realização de cópias de segurança atualizadas e segregadas de forma automática em local protegido, de forma que permita a investigação de incidentes.

Realizar a guarda, preservação ou eliminação de cópias de segurança seguindo tempo de retenção estabelecido.

Possibilitar a recuperação da perda de dados ou sistemas através das cópias de segurança realizadas.

Realizar testes de recuperação a fim de garantir a efetividade da realização das cópias de segurança.

3. DIRETRIZES

A DIA não garante a cópia de segurança (backup) ou a recuperação de arquivos armazenados localmente nos computadores de mesa (desktop) e notebooks dos usuários ou em quaisquer outros dispositivos fora das áreas de armazenamento disponibilizadas pela DIA, conforme disposto na norma de uso aceitável de ativos.

As cópias de segurança em formato eletrônico pertencentes a ativos e/ou recursos de TIC do PJMA, mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deverão estar garantidas nos acordos ou contratos que formalizam a relação entre os envolvidos.

As rotinas de cópia de segurança deverão ser orientadas para a restauração dos

arquivos no menor tempo possível, principalmente quando da indisponibilidade de ativos e/ou recursos de TIC, e utilizarão soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

As rotinas da cópia de segurança deverão possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TIC ou dado armazenado, dando prioridade aos ativos e/ou recursos de TIC críticos do PJMA.

O armazenamento da cópia de segurança deverá ser mantido, preferencialmente, em um local distinto do ambiente principal de TIC. É desejável que se tenha um local remoto ao do ambiente principal de TIC para armazenar cópias de segurança extras dos principais serviços e informações que sejam considerados críticos.

A infraestrutura de rede das cópias de segurança será segregada, lógica e fisicamente, dos sistemas críticos do PJMA. E, deverá ser mantida a reserva de recursos para realização de testes de restauração da cópia de segurança das informações.

Em situações em que a confidencialidade é importante, convém que as cópias de segurança sejam protegidas através de criptografia.

4. FREQUÊNCIA E RETENÇÃO

As cópias de segurança do PJMA deverão ser realizadas utilizando-se as seguintes frequências temporais:

I - diária;

II - semanal;

III - mensal;

IV - anual;

V - temporalidade especial, a depender de necessidades específicas.

As cópias de segurança deverão ser mantidas sob um padrão mínimo, o qual deverá observar a correlação da frequência e da retenção estabelecidos. As especificidades das cópias de segurança poderão demandar frequência e tempo de retenção diferenciados.

Os ativos de TIC envolvidos no processo da cópia de segurança são considerados críticos para o PJMA.

A cópia de segurança dos arquivos eletrônicos produzidos na rede de dados corporativa do PJMA será realizada pela DIA, considerando os requisitos de serviço, de segurança da informação e de proteção de dados envolvidos, bem como a criticidade da informação para a continuidade da operação do PJMA, e deverá explicitar, no mínimo, os seguintes requisitos técnicos:

I - escopo (arquivos eletrônicos internos, base de dados, máquinas virtuais, sistemas, etc.);

II - tipo da cópia de segurança (completa, incremental, diferencial);

III - frequência temporal de realização da cópia de segurança (diária, semanal, mensal, anual, etc.);

IV - tempo de retenção individual, conforme escopo definido;

V - Recovery Point Objective - RPO: diz respeito à quantidade de informação que é tolerável perder, no caso de uma parada nas operações;

VI - Recovery Time Objective - RTO: diz respeito à quantidade de tempo que as operações levam para voltar ao normal, após uma parada.

Os(As) administradores(as) das cópias de segurança da informação deverão zelar pelo cumprimento das diretrizes dos tempos de retenção estabelecidos em procedimento interno da DIA.

A retenção dos dados deverá observar, no que couber, os prazos definidos no Plano de Classificação e Tabelas de Temporalidade do PJMA, que constam na Resolução GP nº 31/2015 ou posterior que a substitua.

5. TIPOS DE CÓPIA DE SEGURANÇA

Existem alguns tipos de cópia de segurança devendo ser observadas as seguintes opções adotadas pelo PJMA:

I - completa (*full*);

II - incremental;

III - diferencial.

6. USO DA REDE

Os(As) administradores(as) das cópias de segurança da informação deverão considerar o impacto da execução das rotinas de cópias sobre o desempenho da rede de dados corporativa e dos serviços, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais ativos e/ou recursos de TIC do PJMA.

A execução das cópias de segurança deverá considerar, preferencialmente, os períodos estabelecidos e as informações de frequência e tipo para realização das mesmas.

O período de realização das cópias de segurança será determinado pelos administradores(as) das cópias em procedimento interno detalhado.

7. TRANSPORTE E ARMAZENAMENTO

As unidades de armazenamento utilizadas na preservação dos dados deverão considerar as seguintes características:

I - a criticidade dos dados armazenados;

II - o tempo de retenção dos dados;

III - a probabilidade de necessidade de restauração;

IV - o tempo esperado para restauração;

V - o custo de aquisição da unidade de armazenamento de cópia de segurança (backup);

VI - a vida útil da unidade de armazenamento da cópia de segurança.

Poderão ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de restauração dos mesmos seja considerado aceitável pelos(as) administradores(as) das cópias de segurança da informação.

A execução das rotinas de cópias de segurança da informação deverá envolver a previsão de ampliação da capacidade dos ativos de TIC envolvidos no armazenamento.

As unidades de armazenamento das cópias de segurança serão acondicionadas em locais apropriados, com proteções físicas implementadas contra: incêndio, inundação, umidade, poeira, pressão, descarga elétrica, explosão, campos eletromagnéticos, etc. e com acesso restrito a servidores(as) da DIA devidamente autorizados(as). Além disso, as condições ambientais deverão estar alinhadas com aquelas descritas pelo fabricante das unidades de armazenamento.

Quando da necessidade de descarte de unidades de armazenamento das cópias de segurança, tais recursos serão fisicamente destruídos, atentando-se aos procedimentos de descarte seguro do PJMA.

As mídias de armazenamento (fitas magnéticas, discos rígidos externos e outras) contendo as cópias de segurança deverão ser transportadas e armazenadas seguindo as orientações abaixo:

I - a mídia será identificada e armazenada em área segura acessível apenas para servidores(as) da DIA devidamente autorizados(as);

II - a mídia não será deixada sem supervisão durante o transporte;

III - as cópias de segurança completas diárias, semanais, mensais e anuais serão mantidas pelo período e local informados em procedimento interno da DIA.

8. TESTES DAS CÓPIAS DE SEGURANÇA

As cópias de segurança da informação serão verificadas periodicamente e deverão ser observada as seguintes orientações:

I - os registros de eventos (logs) das cópias de segurança da informação serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho da cópia de segurança;

II - ações corretivas serão tomadas quando problemas nas cópias de segurança forem identificados, a fim de reduzir os riscos associados a cópias com falha;

III - os registros de eventos (logs) das cópias de segurança e testes de restauração serão mantidos para demonstrar conformidade com esta norma.

Os testes de restauração das cópias de segurança deverão ser realizados, por amostragem, uma vez a cada 2 (duas) semanas, atendendo aos ambientes de

homologação e produção de forma alternada, observados os recursos de TIC disponíveis, a fim de verificar que as cópias de segurança foram bem-sucedidas.

Os registros deverão conter, no mínimo, o tipo de sistema/serviço que teve o seu restabelecimento testado, a data da realização do teste, o tempo gasto para o retorno da cópia de segurança e se o procedimento foi concluído com sucesso, avaliando se foram atendidos os níveis de serviço pactuados, tais como os Recovery Time Objective – RTOs, levando em consideração os diferentes tipos de ambiente (produção, homologação, etc.) do PJMA e os recursos de TIC disponíveis para cada ambiente.

Os registros deverão conter, no mínimo, o tipo de sistema/serviço que teve o seu restabelecimento testado, a data da realização do teste, o tempo gasto para o retorno da cópia de segurança e se o procedimento foi concluído com sucesso, avaliando se foram atendidos os níveis de serviço pactuados, tais como os Recovery Time Objective – RTOs e considerando os diferentes tipos de ambiente (produção, homologação, etc.) do PJMA e os recursos de TIC disponíveis para cada ambiente.

9. RESTAURAÇÃO DE CÓPIA DE SEGURANÇA

Os(As) administradores(as) das cópias de segurança da informação terão a prerrogativa de negar a restauração de dados cujo conteúdo não seja condizente com as atividades laborais, cabendo recurso da negativa ao superior imediato(a) ou gestor(a) da unidade administrativa ou judicial.

O atendimento de solicitações de restauração de cópias deverá obedecer a um processo de restauração, que será definido em procedimento interno detalhado.

A recuperação de mensagens e arquivos eletrônicos da rede corporativa e do ambiente colaborativo deverá ser solicitada para a DIA, através dos canais oficiais de comunicação ou solicitação pelo(a) superior imediato(a) ou gestor(a) da unidade administrativa ou judicial.

9.1 Área de Armazenamento de Arquivos Interna

Os arquivos eletrônicos armazenados na rede corporativa de dados do PJMA, na área disponibilizada pela DIA, que forem excluídos pelo(a) usuário(a) terão possibilidade de recuperação em até 30 (trinta) dias, a contar da data da exclusão dos mesmos.

A restauração de arquivos eletrônicos dos(as) usuários(as), armazenados na rede corporativa do PJMA, somente poderá ser realizada caso tenham sido incluídos na rotina de cópia de segurança do dia anterior.

9.2 Área de Armazenamento de Arquivos Externa (Nuvem)

As mensagens e os arquivos eletrônicos produzidos ou recebidos no ambiente colaborativo fornecido pelo PJMA que forem excluídos pelo(a) usuário(a), deverão observar as orientações abaixo:

I - o(a) próprio(a) usuário(a) poderá recuperar suas mensagens e arquivos eletrônicos em até 30 (trinta) dias quando colocados na lixeira;

II - o(a) administrador(a) de cópias de segurança terá até 25 (vinte e cinco) dias para recuperar as mensagens e arquivos eletrônicos excluídos da lixeira, a contar da data de exclusão, após ação de “esvaziar a lixeira” executada manualmente pelo(a) usuário(a).

Decorrido os prazos dos itens acima, as mensagens e arquivos eletrônicos serão automaticamente apagados pelo serviço do ambiente colaborativo e não terão mais possibilidade de recuperação. Apenas as mensagens e os arquivos eletrônicos dos(as) magistrados(as) ou das unidades administrativas e/ou judiciais poderão ser restaurados após os prazos informados acima.

Caso uma credencial de acesso ao e-mail seja excluída, observado os prazos de bloqueio e exclusão dispostos na norma de controle de acesso e gestão de identidade, o(a) administrador(a) de cópias de segurança poderá recuperar as mensagens e os arquivos eletrônicos do(a) usuário(a) em até 20 (vinte) dias a contar da data de exclusão desta credencial.

10. DO DESCARTE DA MÍDIA

A mídia da cópia de segurança será retirada e descartada conforme descrito neste documento:

I - assegurar que a mídia não contenha mais dados da cópia de segurança ativas e que o conteúdo, atual ou anterior, não possa ser lido ou recuperado por pessoas não autorizadas;

II - garantir a destruição física e lógica da mídia antes do descarte.

11. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

11.1 Diretoria de Informática e Automação

É responsabilidade da Diretoria de Informática e Automação prover ativos e/ou recursos de TIC, a fim de sustentar a gestão das cópias de segurança da informação do PJMA.

11.1.1 Administradores(as) das cópias de segurança da informação

Os(As) administradores(as) das cópias de segurança da informação deverão ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de cópia de segurança. São atribuições dos(as) administradores(as):

I - gerir a(s) ferramenta(s) que realiza(m) as cópias de segurança da informação do PJMA;

II - realizar cópias de segurança da informação dos dados produzidos ou custodiados pelo PJMA;

III - gerir as cópias de segurança da informação, através da guarda, preservação, restauração e descarte seguro das mesmas;

IV - manter as unidades de armazenamento das cópias de segurança preservadas, funcionais e seguras;

V - definir procedimentos que envolvem os processos de cópias e restauração de segurança da informação;

VI - realizar testes de restauração das cópias de segurança;

VII - observar os registros de eventos (logs) das cópias de segurança da informação do PJMA.

12. INFRAÇÕES E PENALIDADES

Infrações e penalidades serão aplicadas conforme previsto na Política de Segurança da Informação.

13. REVISÕES

Esta norma será alterada mediante necessidade de atualização, com apreciação e aprovação do Comitê de Governança de Segurança da Informação (CGSI).

14. APROVAÇÃO

A norma foi aprovada pelo Comitê de Governança de Segurança da Informação (CGSI), revogando-se todas as disposições em contrário.

ANEXO IX

NORMA DE GESTÃO DE CRIPTOGRAFIA E GERENCIAMENTO DE CHAVES

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo
Resolução nº 27/2013-GP	
PORTARIA nº 97/2019-GP	

Versionamento:

Versão:	1.0
Data:	02/05/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	24/07/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

1. INTRODUÇÃO

A norma de gestão de criptografia e gerenciamento de chaves complementa a Política de Segurança da Informação (PSI), definindo as diretrizes para garantir o acesso aos ativos Tecnologia da Informação e Comunicação (TIC) ou Sistemas de Informação do Poder Judiciário do Estado do Maranhão (PJMA) com níveis adequados de proteção.

Para fins desta norma, aplica-se a lista de termos do glossário com suas respectivas definições, conforme descrito no ANEXO I da PSI.

Esta norma obedece ao escopo definido na Política de Segurança da Informação, estabelecendo regras sobre o uso efetivo e adequado de criptografia na proteção da informação.

2. OBJETIVO

Assegurar o uso adequado e eficaz da criptografia para proteger a confidencialidade, autenticidade e integridade das informações de acordo com os requisitos de segurança da informação da organização, levando em consideração os requisitos legais, estatutários, regulamentares e contratuais relacionados à criptografia.

3. DIRETRIZES

É vedada a implantação de controles criptográficos não homologados pelo Poder Judiciário do Estado do Maranhão. Os controles criptográficos serão usados para assegurar:

I - a confidencialidade, a integridade e a autenticidade de informações sensíveis ou críticas que se encontrem armazenadas ou sob processo de transmissão eletrônica;

II - o não-repúdio: provar a ocorrência de evento ou ação alegados e suas entidades participativas originárias, de forma a resolver disputas sobre a ocorrência ou não de evento ou ação e do envolvimento ou não destas entidades;

III - a autenticação: confirmar a identidade de usuários ou de sistemas automatizados.

A escolha dos tipos, da qualidade e da força de algoritmos, assim como a definição de que tipo de controle criptográfico é apropriado para cada propósito e

processo de negócio, tomará como base, sempre que possível, o resultado do processo de gerenciamento de riscos de segurança da informação.

Os computadores de mesa e dispositivos móveis (notebooks) dos(as) desembargadores(as), juízes(as), diretores(as) e/ou presidente contendo dados confidenciais deverão ser criptografados por ferramenta disponibilizada ou autorizada pela DIA, podendo optar pela criptografia a nível de disco, pasta ou arquivo.

Os dispositivos de armazenamento removíveis (pendrives e discos rígidos externos, etc.), de uso exclusivamente corporativo, dos(as) usuários(as) contendo dados confidenciais deverão ser criptografados por ferramenta disponibilizada ou autorizada pela DIA, devendo optar pela criptografia a nível de dispositivo.

Os dados sensíveis disponíveis em servidores de rede, sistemas e bancos de dados poderão ser criptografados, após a devida avaliação da DIA.

A segurança dos dados que trafegam na rede corporativa ou na internet, como credenciais de acesso e informações sensíveis, deverão utilizar mecanismos de criptografia, tais como: Transport Layer Security (TLS) e Open Secure Shell (OpenSSH).

4. CERTIFICADOS DIGITAIS

Os certificados digitais utilizados no âmbito do Poder Judiciário do Estado do Maranhão serão adquiridos de autoridade certificadora credenciada pela ICP-Brasil, para identificar servidores de rede e sistemas de uso interno, para substituir credenciais de acesso de usuários(as) baseadas em login e senha utilizadas nos sistemas administrativos ou judiciais ou para assinar documentos eletrônicos, bem como documentos reproduzidos em meio eletrônico gerados no PJMA.

Os certificados digitais e os suportes criptográficos (tokens) serão cedidos aos(às) usuários(as) que necessitarem utilizar a assinatura digital em razão do exercício das atribuições do cargo ou função pública que ocuparem.

O certificado digital é de uso pessoal e intransferível, cabendo ao(à) usuário(a) zelar pela confidencialidade da senha, bem como pela guarda e pela conservação do suporte criptográfico (token), sob pena de responsabilidades cíveis, penais ou administrativas cabíveis, assegurado o contraditório e a ampla defesa.

Para emissão e uso do certificado digital, os(as) usuários(as) do PJMA deverão observar a PORTARIA-GP - 972019 ou posterior que a substitua e a Resolução nº 272013-GP ou posterior que a substitua.

5. GERENCIAMENTO DE CHAVES

O gerenciamento de chaves do PJMA deverá garantir a confidencialidade, integridade e disponibilidade das chaves criptográficas, além de proteger as chaves contra acesso não autorizado, perda, roubo ou comprometimento, garantindo a conformidade com as leis e regulamentações aplicáveis.

O PJMA deverá dispor de um gerador de chaves criptográficas seguro e confiável e designar uma equipe responsável pelo gerenciamento das chaves criptográficas, bem como controle de acesso adequado para restringir o acesso a estas chaves.

A realização de cópias de segurança (backup) das chaves criptográficas deverá ser realizada de forma regular e segura. Garantindo que as cópias de segurança estejam armazenadas em um local separado do armazenamento principal, devendo ser testado regularmente a restauração das chaves a partir das cópias de segurança para garantir a sua integridade. Para recuperação das chaves criptográficas, em caso de perda ou comprometimento, a DIA adotará procedimento específico.

O PJMA deverá manter um registro das chaves geradas e distribuídas para fins de auditoria e possível responsabilização dos(as) usuários(as) autorizados(as) pela DIA.

6. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

6.1 Usuários(as)

Além do disposto na Resolução GP nº 31/2015 ou posterior que a substitua, compete ao(à) usuário(a):

I - estar de posse do certificado digital para o desempenho de atividades profissionais que requeiram o uso deste;

II - solicitar à autoridade certificadora, de acordo com procedimentos definidos para esse fim, a imediata revogação do certificado em caso de inutilização, observando as situações dispostas na Resolução GP nº 27/2013 ou posterior que a substitua;

III - alterar imediatamente a senha de acesso do certificado digital em caso de suspeita de seu conhecimento por pessoa não autorizada;

IV - observar as diretrizes de complexidade e tamanho definidas para elaboração de senhas, dispostas na norma de controle de acesso e gestão de identidade, para criação de senha do certificado digital;

V - manter o suporte criptográfico (token) em local seguro e com proteção física contra acesso indevido, descargas eletromagnéticas, calor e/ou umidade excessivos e outras condições ambientais que representem risco à integridade das mesmas;

VI - solicitar o fornecimento de novo suporte criptográfico (token) ou certificado digital nos casos de inutilização, revogação ou expiração da validade do certificado, observando as situações dispostas na Resolução GP nº 27/2013 ou posterior que a substitua;

VII - verificar periodicamente a data de validade do certificado digital e solicitar tempestivamente a emissão de um novo, conforme orientações expedidas para esse fim;

VIII - devolver em boas condições o suporte criptográfico (token) anteriormente cedido em caso de desligamento do quadro de pessoal do PJMA.

Em caso de perda, roubo ou furto do suporte criptográfico (token), o(a) usuário(a) deverá procurar a ajuda das autoridades policiais registrando boletim de ocorrência e em seguida comunicar, via DIGIDOC, a Diretoria de Informática e Automação para que possam ser tomadas as medidas cabíveis.

6.2 Diretoria de Informática e Automação

Compete à Diretoria de Informática e Automação:

I - realizar a gestão dos certificados digitais e suportes criptográficos (tokens) utilizados no PJMA;

II - adequar a infraestrutura de TIC para uso dos certificados digitais;

III - elaborar e divulgar padrões de compatibilidade dos certificados digitais e dos respectivos suportes criptográficos utilizados no PJMA;

IV - desenvolver em sua área de atuação novas aplicações, ou atualizar as existentes, que requeiram a utilização de certificados digitais;

V - elaborar e divulgar procedimentos para recuperação de informações criptografadas, no caso de chaves perdidas, comprometidas ou danificadas;

VI - tomar medidas administrativas a respeito dos suportes criptográficos (tokens) que tenham sido objetos de perda, roubo ou furto, reportando, no que couber, as Diretorias Administrativa e/ou a de Segurança Institucional e Gabinete Militar.

6.3 Diretoria Administrativa

Compete à Diretoria Administrativa:

I - realizar acompanhamento administrativo junto a DIA a respeito dos suportes criptográficos (tokens) que tenham sido objetos de perda, roubo ou furto.

6.4 Diretoria de Segurança Institucional e Gabinete Militar

Compete à Diretoria de Segurança Institucional e Gabinete Militar:

I - fornecer apoio técnico, por meio de sistema de segurança eletrônica e outros recursos disponíveis, para investigações em andamento de possíveis ilícitos relacionados aos suportes criptográficos (tokens) nas dependências do PJMA.

7. INFRAÇÕES E PENALIDADES

Infrações e penalidades serão aplicadas conforme previsto na Política de Segurança da Informação.

8. REVISÕES

Esta norma será alterada mediante necessidade de atualização, com apreciação e aprovação do Comitê de Governança de Segurança da Informação (CGSI).

9. APROVAÇÃO

A norma foi aprovada pelo Comitê de Governança de Segurança da Informação (CGSI), revogando-se todas as disposições em contrário.

ANEXO XII
NORMA DE DESENVOLVIMENTO SEGURO

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo
Resolução nº 5/2017-GP	
Portaria nº 3/2021-DIA	

Versionamento:

Versão:	1.0
Data:	02/05/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	24/07/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

1. INTRODUÇÃO

Esta norma complementa a Política de Segurança da Informação (PSI), definindo as diretrizes para desenvolvimento seguro e manutenção de todos os serviços, arquitetura, software e sistemas que fazem parte do Poder Judiciário do Estado do Maranhão (PJMA).

Para fins desta norma aplica-se a lista de termos do glossário com suas respectivas definições, conforme descrito no ANEXO I da PSI.

Esta norma obedece ao escopo definido na Política de Segurança da Informação.

A equipe da Coordenadoria de Sistema de Informação (CSI) nesta norma será representada pelos(as) servidores(as), terceirizados(as), prestadores(as) de serviço e estagiários(as) lotados(as) na própria Coordenadoria subordinada à Diretoria de Informática e Automação (DIA) do Poder Judiciário do Estado do Maranhão.

Esta norma se estenderá a outras unidades judiciais ou administrativas do PJMA que estejam envolvidas no desenvolvimento de sistemas ou aplicações.

Somente os sistemas e softwares homologados pela Diretoria de Informática e Automação poderão ser utilizados no âmbito do PJMA.

2. OBJETIVOS

Garantir que a segurança da informação seja implementada em todo ciclo de vida de desenvolvimento dos sistemas de informação.

Atender aos princípios e requisitos de segurança da informação para sistemas de informação adquiridos pelo TJMA.

Atender aos princípios e requisitos de segurança da informação para sistemas de informação mantidos e/ou desenvolvidos pela equipe de sistemas do TJMA ou por terceirizados e/ou contratados supervisionados pela equipe de sistemas do TJMA.

Adotar práticas e requisitos de segurança cibernética no desenvolvimento de projetos novos ou em desenvolvimento, tais como ativação do Múltiplo Fator de Autenticação (MFA).

3. DIRETRIZES

Orientações da norma de desenvolvimento seguro.

3.1 Requisitos de Segurança da Aplicação

Ao desenvolver, ou adquirir novos sistemas de informação ou alterar os existentes, a CSI deverá identificar e especificar os requisitos de software por meio de uma avaliação de risco, de modo que seja avaliado, no mínimo, os seguintes itens:

I - os riscos relacionados ao acesso não autorizado ao ambiente de desenvolvimento;

II - os riscos relacionados a mudanças não autorizadas no ambiente de desenvolvimento;

III - vulnerabilidades técnicas dos sistemas de TIC utilizados no PJMA, contendo relatórios e um processo de entrada, atribuição, correção e teste da correção das vulnerabilidades;

IV - os riscos que uma nova tecnologia pode trazer caso utilizada no PJMA.

3.2 Requisitos de Segurança Relacionados às Redes Públicas

A DIA será responsável pela definição de controles de segurança relacionados às informações em serviços de aplicativos que passam pelas redes públicas:

I - a descrição dos sistemas de autenticação a ser utilizados;

II - a descrição de como confidencialidade e integridade das informações deverão ser assegurados;

III - a descrição de como o não repúdio de ações será assegurado.

3.3 Princípios de Desenvolvimento Seguro

A DIA deverá proteger todos os componentes do software contra adulteração e/ou acesso não autorizado, gerenciando o controle de acesso adequado para proteger os arquivos relacionados ao desenvolvimento. Isso inclui atribuir permissões específicas a usuários(as) ou grupos de usuários(as), limitando o acesso apenas aos desenvolvedores autorizados. Além disso, o princípio do menor privilégio deverá ser aplicado, concedendo apenas as permissões necessárias para cada desenvolvedor.

A CSI deverão produzir software seguro que tenha vulnerabilidades de

segurança mínimas em suas aplicações ou sistemas, levando em consideração as boas práticas de desenvolvimento seguro, tais como ativação do Múltiplo Fator de Autenticação (MFA) e utilização de Single Sign-On (SSO).

Para análise de segurança do código fonte, a CSI poderá fazer o uso de uma ferramenta de análise estática para verificar automaticamente o código em busca de vulnerabilidades e conformidade com os padrões de codificação segura. Esta ferramenta deverá ser utilizada para corrigir práticas de software inseguras documentadas e verificadas continuamente.

A CSI, sempre que necessário, poderá utilizar bibliotecas e/ou componentes de software de terceiros atualizados e confiáveis. E, obrigatoriamente, selecionará frameworks estabelecidos no mercado e comprovadamente seguros.

A CSI deverá aplicar princípios de design seguro em arquiteturas de aplicativos, seguindo as melhores práticas do mercado, como exemplo o projeto OWASP (Open Web Application Security Project).

A CSI deverá conduzir a modelagem de ameaças, sendo conduzido por pessoas especialmente treinadas que avaliam o design da aplicação e medem os riscos de segurança para cada ponto de entrada e nível de acesso.

3.4 Ambiente de Desenvolvimento

As aplicações desenvolvidas pelo PJMA, deverão possuir separação adequada quanto aos sistemas de desenvolvimento, homologação e produção e operação deles em diferentes domínios (por exemplo, em ambientes virtuais ou físicos separados).

As informações sensíveis, como dados pessoais, utilizadas nos ambientes de desenvolvimento e de homologação dos sistemas de informação deverão ser evitadas, substituindo-os, sempre que possível, por dados fictícios ou anonimizados.

3.5 Ambiente de Homologação

As alterações nas aplicações deverão ser validadas formalmente, pelos(as) usuários(as) final(is) e pela equipe técnica, no ambiente de homologação antes de serem aplicadas no ambiente de produção.

Dados confidenciais, bem como dados que podem estar relacionados a informações pessoais e protegidos pela LGPD não deverão ser utilizados nos ambientes de desenvolvimento e homologação. As exceções serão aprovadas pelo Comitê Gestor de Proteção de Dados Pessoais (CGPD), cabendo à DIA definir como

estes dados serão protegidos.

A DIA será responsável por definir a metodologia, as responsabilidades e o tempo de verificação se todos os requisitos de segurança da informação foram cumpridos e se o sistema é aceitável para a produção.

3.6 Treinamentos

A DIA deverá:

I - certificar-se de que todo o pessoal de desenvolvimento de software receba treinamento para escrever código seguro, incluindo princípios gerais de segurança e práticas padrão de segurança de aplicativos;

II - garantir treinamentos que promovam a segurança dentro da equipe de desenvolvimento e construam uma cultura de segurança entre os desenvolvedores.

A CSI definirá o nível de habilidades de segurança e conhecimentos necessários para o processo de desenvolvimento seguro dos treinamentos propostos.

A CSI deverá editar procedimentos baseado em boas práticas de desenvolvimento seguro para os sistemas de informações, tanto para o desenvolvimento de novos sistemas quanto para a manutenção dos sistemas existentes, bem como definirá as normas mínimas de segurança que deverão ser cumpridas.

Os mesmos princípios de desenvolvimento seguro serão aplicados para sistemas de informação mantidos e/ou desenvolvidos por terceirizados e/ou contratados supervisionados pela equipe de sistemas do TJMA.

3.7 Repositórios

Os códigos-fonte deverão ser hospedados em repositórios internos cedidos pelo PJMA. Os repositórios remotos, tais como GitHub, GitLab ou Bitbucket só deverão ser utilizados caso seja devidamente autorizado pela DIA.

O acesso aos repositórios deverá ser protegido por autenticação de dois fatores (2FA) e outras medidas de segurança, como utilização de senhas fortes.

Dependendo da sensibilidade do código ou de outros arquivos relacionados ao desenvolvimento, a CSI poderá criptografá-los para impedir o acesso não autorizado,

que pode ser alcançado por meio de criptografia de disco, criptografia de arquivo ou criptografia de transporte, seguindo as diretrizes da norma de gestão de criptografia e gerenciamento de chaves do PJMA.

3.8 Controle de Versão (Versionamento)

A CSI poderá utilizar o sistema de controle de versão (numeração, datas, etc.) e aplicar nos ambientes de desenvolvimento, homologação e/ou produção. Este sistema permite que várias pessoas trabalhem em conjunto, rastreiem as alterações feitas no código ao longo do tempo e revertam para versões anteriores, caso seja necessário.

Todos os sistemas de informação próprios e de terceiros, terão suas diversas versões disponibilizadas em ciclos de desenvolvimento, homologação e/ou produção, denominados de lançamentos (releases). Os lançamentos serão disponibilizados em intervalos fixos mínimos de 30 dias na maioria dos casos, podendo ocorrer em intervalos menores caso haja necessidade expressa da administração.

Toda e qualquer alteração não emergencial nos sistemas de informação deverá ser incluída no próximo lançamento, de acordo com a capacidade operacional da DIA e seguindo ordem de priorização definida pela CSI.

A cada ciclo de desenvolvimento, a Diretoria de Informática e Automação informará sua capacidade operacional, a fim de suportar a priorização de suas demandas e determinada pelos seguintes fatores:

I - número de homem/horas disponíveis para cada lançamento;

II - demandas emergenciais impostas por alterações legais ou normativas, pelo Conselho Nacional de Justiça (CNJ) ou pela equipe técnica da DIA;

III - projetos definidos no Planejamento Estratégico do Tribunal;

IV - correção emergencial de erros dos sistemas de informação em uso;

V - projetos definidos como prioritários pela DIA ou pela Presidência do Tribunal de Justiça do Maranhão.

A Diretoria de Informática e Automação efetuará catalogação dos sistemas de informação em uso no Poder Judiciário do Maranhão, categorizando-os em:

I – operacionais;

II – táticos;

III – estratégicos.

3.9 Cópias de Segurança

Os sistemas de informações do PJMA deverão ter cópias de segurança (backup) regulares dos arquivos relacionados ao desenvolvimento, para evitar perda de dados em casos de incidentes de segurança da informação, tais como, falhas de hardware, desastres naturais ou ataques cibernéticos. As cópias de segurança deverão ser armazenadas em locais seguros e testados regularmente para garantir sua integridade e capacidade de recuperação, seguindo as diretrizes da norma de cópias de segurança da informação.

3.10 Controle de Alterações

As alterações no desenvolvimento e as manutenções dos sistemas de informação do PJMA deverão ser realizadas observando o disposto na PORTARIA-DIA nº 3/2021 ou posterior que a substitua.

O Diretor de Informática e Automação poderá, a seu critério, autorizar alterações emergenciais no desenvolvimento e na manutenção dos sistemas de informação do PJMA.

4. NOVOS SISTEMAS DE INFORMAÇÃO

A implementação de novos sistemas de informação adquiridos, recebidos em doação, ou desenvolvidos internamente, está condicionada a análise prévia de viabilidade técnica, a ser realizada por dois servidores efetivos da Diretoria de Informática e Automação.

A análise de viabilidade técnica deverá produzir um Relatório de Diagnóstico de Sistema, elaborado e assinado por 02 (dois) servidores efetivos da DIA, que analisará a adequação do sistema proposto ao ambiente computacional do PJMA e recomendará a continuidade ou cancelamento do processo de implementação, sempre considerando questões relacionadas à segurança da informação e privacidade de dados pessoais.

A Coordenadoria de Sistemas de Informação da Diretoria de Informática e Automação deverá emitir parecer técnico sobre a aquisição ou desenvolvimento de novos sistemas ou a realização de manutenções evolutivas e corretivas em sistemas já existentes, necessárias para cumprimento do ato administrativo.

5. PAPÉIS E RESPONSABILIDADES

É obrigatório o uso dos sistemas de informação do PJMA por magistrados(as) e servidores(as), cabendo-lhes incluir, de forma fidedigna e tempestiva, todas as informações processuais e administrativas, possibilitando maior transparência e celeridade aos métodos e procedimentos processuais utilizados.

5.1 Diretoria de Informática e Automação

Compete exclusivamente à DIA:

I – gerir os softwares e os sistemas de informação do PJMA;

II – homologar sistemas de informação para uso nas atividades jurisdicionais e administrativas;

III – desenvolver ou adquirir sistemas de informação buscando sempre dar celeridade às atividades jurisdicionais ou administrativas;

IV – aplicar atividades de perícia e auditoria de operações realizadas nos sistemas de informação;

V – aplicar políticas de homologação de softwares e/ou sistemas;

VI – aplicar mecanismos de controle de licenças de uso e bloqueio de instalações de softwares não licenciados ou não homologados;

VII – aplicar políticas de controle de alterações das configurações dos sistemas.

O uso não autorizado de software de propriedade intelectual do PJMA, para atividades como reprodução, modificação, distribuição ou qualquer outra forma de uso das aplicações sem permissão expressa da DIA, será proibido.

5.2 Comitê Gestor de Proteção de Dados Pessoais

São responsabilidades do CGPD:

I - aprovar o uso de dados confidenciais e dados pessoais protegidos pela LGPD nos ambientes de desenvolvimento e homologação.

6. INFRAÇÕES E PENALIDADES

Infrações e penalidades serão aplicadas conforme previsto na Política de Segurança da Informação.

7. REVISÕES

Esta norma será alterada mediante necessidade de atualização, com apreciação e aprovação do Comitê de Governança de Segurança da Informação (CGSI).

8. APROVAÇÃO

A norma foi aprovada pelo Comitê de Governança de Segurança da Informação (CGSI), revogando-se todas as disposições em contrário.

ANEXO XVII
NORMA DE GESTÃO DE SERVIÇOS EM NUVEM

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo

Versionamento:

Versão:	1.0
Data:	02/05/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	24/07/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

1. INTRODUÇÃO

A norma de gestão de serviços em nuvem dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelo Poder Judiciário do Estado do Maranhão (PJMA).

Para fins desta norma, aplica-se a lista de termos do glossário com suas respectivas definições, conforme descrito no ANEXO I da PSI.

Esta norma obedece ao escopo definido na Política de Segurança da Informação.

2. OBJETIVO

Especificar e gerenciar a segurança da informação para o uso de serviços em nuvem.

3. DIRETRIZES

Orientações da norma de gestão de serviços em nuvem.

3.1 REQUISITOS PARA A ADOÇÃO SEGURA DE COMPUTAÇÃO EM NUVEM

A computação em nuvem é composta pelos seguintes modelos de implantação:

I - nuvem privada (ou interna);

II - nuvem comunitária;

III - nuvem pública (ou externa); e

IV - nuvem híbrida.

Para que o PJMA adote soluções de computação em nuvem de forma segura, com o objetivo de elevar o nível de proteção das informações no uso dessa tecnologia, deverão ser observados alguns requisitos mínimos que serão vistos a seguir.

3.1.1 Transferência de Serviços para um Provedor de Serviço de Nuvem

Antes de transferir serviços ou informações para um provedor de serviço de nuvem, o PJMA deverá, no mínimo:

I - garantir que estejam alinhadas à legislação brasileira e aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros;

II - realizar o gerenciamento de riscos, precedido por análise e relatório de impacto de dados pessoais, em conformidade com a legislação;

III - definir o modelo de serviço e de implementação de computação em nuvem que será adotado;

IV - avaliar quais informações serão hospedadas na nuvem;

V - definir as medidas de mitigação de riscos e de custos para a implementação de solução de computação em nuvem e para possibilidade de crescimento dessa solução;

VI - planejar custos de migração das informações e dos serviços, nos casos de ingresso e de saída do serviço de computação em nuvem.

3.1.2 Capacidade do Provedor de Serviço de Nuvem para Implementar Atualizações

Em função da capacidade do provedor de serviço de nuvem implementar atualizações relacionadas à segurança da informação em seus produtos e serviços, o PJMA deverá, no mínimo:

I - definir os critérios e a periodicidade das atualizações dos procedimentos e dos recursos computacionais a serem observados pelo provedor de serviço de nuvem;

II - revisar e atualizar periodicamente seus processos internos de gestão de riscos de segurança da informação.

3.1.3 Gerenciamento de Identidades e de Registros de Eventos (Logs)

Em relação ao gerenciamento de identidades e de registros, o PJMA deverá, no mínimo:

I - adotar padrão único de identidade para permitir o uso de tecnologia Single

Sign-On (SSO) no processo de autenticação de seus(suas) usuários(as) no provedor de serviço de nuvem;

II - gerir junto ao provedor de serviço de nuvem o acesso ao ambiente de autenticação do PJMA;

III - adotar, de acordo com o nível de criticidade da informação, o uso da tecnologia SSO, o qual deverá ser acompanhado de Múltiplo Fator de Autenticação (MFA) ou de outra alternativa que aumente o grau de segurança no processo de autenticação de seus(suas) usuários(as) no provedor de serviço de nuvem;

IV - exigir do provedor de serviço de nuvem o registro e armazenamento de todos os acessos, incidentes e eventos cibernéticos, incluídas informações sobre sessões e transações e armazene tudo pelo período de 01 (um) ano, no ambiente do provedor de serviço de nuvem ou em ambiente próprio controlado, à critério do PJMA;

V - manter em ambiente próprio controlado, por no mínimo 02 (dois) anos, os registros de todos os acessos, incidentes e eventos cibernéticos, incluindo informação sobre sessões e transações recebidos do provedor de serviço de nuvem;

VI - capacitar os administradores do ambiente em nuvem, para acessar e utilizar os registros gerados pelo provedor de serviço de nuvem.

3.1.4 Uso de Recursos Criptográficos

Em relação à necessidade do uso de recursos criptográficos, o PJMA deverá, no mínimo:

I - verificar se os dados da organização estão sendo tratados e armazenados de acordo com a legislação vigente;

II - analisar a necessidade de criptografar dados com base nos requisitos legais, nos riscos, no nível de criticidade, nos custos e nos benefícios;

III - utilizar, sempre que possível, chaves de criptografia, com tamanho mínimo de 1024 bits, baseadas em suporte criptográfico (token).

3.1.5 Segregação de Dados e da Separação Lógica

Em relação à segregação de dados e à separação lógica em ambientes de computação em nuvem, o PJMA, em conjunto com o provedor de serviço de nuvem, deverão estabelecer, no mínimo, as seguintes ações:

I - garantir que o ambiente contratado seja protegido de usuários(as) externos(as) do serviço em nuvem e de pessoas não autorizadas;

II - implementar controles de segurança da informação de forma a propiciar o isolamento adequado dos recursos utilizados pelo PJMA e por outros(as) usuários(as) do serviço em nuvem;

III - garantir que seja aplicada segregação lógica apropriada dos dados das aplicações virtualizadas, dos sistemas operacionais, do armazenamento e da rede a fim de estabelecer a separação de recursos utilizados;

IV - garantir a separação de todos os recursos utilizados pelo provedor de serviço de nuvem daqueles recursos utilizados pela administração interna do PJMA;

V - avaliar os riscos associados à execução de softwares proprietários a serem instalados no serviço de nuvem.

3.1.6 Tratamento da Informação

Em relação ao tratamento da informação em ambiente de computação em nuvem, o PJMA, além de cumprir as orientações contidas na legislação sobre proteção de dados pessoais, deverá observar as seguintes diretrizes:

I - informação sem restrição de acesso poderá ser tratada em ambiente de nuvem, considerada a legislação e os riscos de segurança da informação;

II - informação classificada como confidencial não poderá ser tratada em ambiente de computação em nuvem;

III - poderão ser tratados em ambiente de computação em nuvem, observados os riscos de segurança da informação e a legislação vigente:

a) a informação com restrição de acesso prevista na legislação;

b) a informação classificada como restrita regulada pelo próprio PJMA.

Os dados, metadados, informações e conhecimentos produzidos ou

custodiados pelo PJMA, transferidos para o provedor de serviço de nuvem, deverão estar hospedados em território brasileiro, observando-se as seguintes disposições:

I - pelo menos uma cópia de segurança deverá ser mantida em território brasileiro;

II - a informação sem restrição de acesso poderá possuir cópias de segurança fora do território brasileiro, conforme legislação aplicável;

III - a informação com restrição de acesso prevista na legislação e a classificada como restrita regulada pelo próprio PJMA, bem como suas cópias de segurança, não poderão ser tratadas fora do território brasileiro;

IV - no caso de dados pessoais, deverão ser observadas as orientações previstas na Lei no 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD, e demais legislações sobre o assunto.

3.1.7 Cláusulas Contratuais

O instrumento contratual a ser firmado com um provedor de serviço de nuvem para a prestação do serviço de computação em nuvem deverá conter, minimamente, além das diretrizes que tratam esta norma, os seguintes procedimentos de segurança:

I - termo de confidencialidade que impeça o provedor de serviço de nuvem de usar, transferir e liberar dados, sistemas, processos e informações do PJMA para empresas nacionais, transnacionais, estrangeiras, países e governos estrangeiros;

II - garantia da exclusividade de direitos, por parte do PJMA, sobre todas as informações tratadas durante o período contratado, incluídas eventuais cópias disponíveis, tais como backups de segurança;

III - proibição do uso de informações do PJMA pelo provedor de serviço de nuvem para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado;

IV - conformidade da política de segurança da informação do provedor de serviço de nuvem com a legislação brasileira;

V - devolução integral dos dados, informações e sistemas sob custódia do provedor de serviço de nuvem ao PJMA no término do contrato;

VI - eliminação, por parte do provedor de serviço de nuvem, ao término do contrato, de qualquer dado, informação ou sistema do PJMA sob sua custódia, observada a legislação que trata da obrigatoriedade de retenção de dados;

VII - garantia do direito ao esquecimento para dados pessoais, conforme art. 16 da Lei no 13.709, de 14 de agosto de 2018 - LGPD.

3.2 DOS REQUISITOS DO PROVEDOR DE SERVIÇO DE NUVEM

Para que esteja habilitado a prestar serviços de computação em nuvem para o PJMA, o provedor de serviço de nuvem deverá cumprir, no mínimo, os seguintes requisitos:

I - possuir metodologia de gestão de riscos, elaborada em conformidade com as melhores práticas e com a legislação, bem como realizar o gerenciamento de riscos descrito na norma de gestão de riscos da segurança da informação;

II - implementar práticas de fortalecimento dos mecanismos de virtualização;

III - possuir processos de gestão de continuidade de negócios e de gestão de mudanças, em conformidade com os normativos existentes e com as melhores práticas nestas áreas;

IV - possuir um plano de recuperação de desastres que estabeleça procedimentos de recuperação e de restauração de plataforma, infraestrutura, aplicações e dados após incidentes de perda de dados;

V - estabelecer um canal de comunicação seguro utilizando, no mínimo, Secure Sockets Layer/Transport Layer Security (SSL/TLS);

VI - utilizar um padrão de criptografia segura, conforme padrão internacional reconhecidamente aceito, que possa ser implementado com chaves criptográficas, com tamanho mínimo de 1024 bits, geradas e armazenadas pelo PJMA;

VII - disponibilizar facilidades que possibilitem a aplicação de uma proteção criptográfica própria do PJMA;

VIII - notificar, imediatamente, ao PJMA incidente cibernético contra os serviços ou dados sob sua custódia;

IX - possuir procedimentos necessários para preservação de evidências, conforme legislação;

X - demonstrar estar em conformidade com os padrões de segurança do serviço em nuvem.

3.2.1 Gerenciamento de Identidades e de Registros de Eventos (Logs)

Em relação ao gerenciamento de identidades e registros o provedor de serviço de nuvem deverá:

I - possuir procedimentos de controle de acesso que abordam a transição entre as funções, os limites e controles dos privilégios dos(as) usuários(as) e os controles de utilização das contas de usuários(as);

II - impor mecanismo de autenticação que exija tamanho mínimo, complexidade, duração e histórico de senhas de acesso;

III - suportar tecnologia SSO para autenticação;

IV - suportar mecanismos de Múltiplo Fator de Autenticação (MFA) ou outra alternativa que aumente o grau de segurança no processo de autenticação de usuários(as) do PJMA no provedor de serviço de nuvem, de acordo com nível de criticidade da informação;

V - permitir ao PJMA gerenciar as próprias identidades, inclusive criação, atualização, exclusão e suspensão no ambiente fornecido pelo provedor de serviço de nuvem;

VI - atender aos requisitos legais, às melhores práticas de segurança e a outros critérios exigidos pelo PJMA em seus processos de autenticação, controle de acesso, contabilidade e de registro (formato, retenção e acesso).

3.2.2 Segurança de Aplicações Web

Em relação à segurança de aplicações web disponibilizadas no ambiente remoto o provedor de serviço de nuvem deverá:

I - utilizar firewalls especializados na proteção de sistemas e aplicações;

II - desenvolver código web em conformidade com as diretrizes da norma de

desenvolvimento seguro do PJMA, além de seguir as melhores práticas aplicadas no mercado;

III - utilizar melhores práticas de segurança de sistemas operacionais e de aplicações;

IV - realizar ou permitir a realização de testes de invasão (pentest) de redes e de aplicações;

V - possuir um programa de análise/correção de vulnerabilidades.

3.2.3 Segregação de dados

Em relação à segregação de dados o provedor de serviço de nuvem deverá:

I - isolar, utilizando separação lógica, todos os dados e serviços do PJMA de outros clientes de serviço em nuvem;

II - segregar o tráfego de gerenciamento do tráfego de dados do PJMA;

III - implementar mecanismos de segurança entre zonas.

3.2.4 Descarte de Ativos de Informação e de Dados

O provedor de serviço de nuvem deverá possuir procedimentos em relação ao descarte de ativos de informação e de dados, que assegurem:

I - sanitizar ou destruir, de modo seguro, os dados existentes nos dispositivos descartados por meio da utilização de métodos que estejam em conformidade com os padrões estabelecidos para a conduta e as melhores práticas;

II - destruir, de modo seguro, ativo de informação no fim do ciclo de vida ou considerado inservível e discriminar os ativos que foram reciclados, bem como o peso e os tipos de materiais obtidos em virtude do processo de destruição;

III - armazenar, de modo seguro, ativos de informação a serem descartados, em ambiente com acesso físico ou lógico controlado, com registro de toda movimentação de entrada e de saída de dispositivos.

3.3 CLOUD BROKER

O cloud broker deverá atuar como integrador dos serviços de computação em nuvem entre o PJMA e dois ou mais provedores de serviço de nuvem.

Caso o PJMA realize contratação por meio do cloud broker, plataforma de gestão de múltiplos serviços de nuvem (multinuvem), para realizar procedimentos de provisionamento e orquestração de ambiente, é necessário que a ferramenta observe as disposições seguintes.

3.3.1 Provisionamento e Orquestração

Em relação às funcionalidades de provisionamento e orquestração de multinuvem, o cloud brokers deverá:

I - provisionar para o(a) usuário(a) final um único portal integrado;

II - utilizar modelos de provisionamento;

III - implementar automação segura de provisionamento simultâneo e utilização, no que couber, ferramentas de código aberto e interoperáveis;

IV - realizar fluxos de trabalho de orquestração baseada em eventos;

V - apresentar soluções seguras integradas de criação de Infraestrutura por Código - IaaC.

3.3.2 Monitoramento e Análise

Com relação às funcionalidades de monitoramento e análise em multinuvem, a plataforma deverá:

I - entregar relatórios de monitoramento de desempenho de recursos na nuvem;

II - realizar coleta e monitoramento dos registros;

III - apresentar procedimentos de monitoramento de alertas.

3.3.3 Inventário e Classificação

Em relação às funcionalidades de inventário e classificação em multinuvem, o cloud brokers deverá:

I - inventariar os recursos na nuvem;

II - apresentar procedimentos de segurança para configuração de recursos na plataforma de gestão multinuvem;

III - detectar recursos sem etiqueta.

3.3.4 Gerenciamento de Segurança, Conformidade e Identidade

Em relação às funcionalidades de gerenciamento de segurança, conformidade e identidade, a plataforma deverá:

I - possuir mecanismos de SSO e de Múltiplo Fator de Autenticação (MFA) das plataformas em nuvem;

II - dispor de gerenciamento seguro de usuários(as) e de grupos de usuários(as);

III - realizar gerenciamento de segurança dos recursos;

IV - apresentar notificações de eventos de alerta multicanal;

V - possuir gerenciamento de identidade e acesso - IAM;

VI - realizar registros de atividades da plataforma em nuvem;

VII - armazenar os dados em datacenter abrigado em território brasileiro;

VIII - cumprir a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD;

IX - atender aos requisitos de disponibilidade, de escalabilidade, de redundância e de criptografia.

O cloud broker poderá utilizar ferramentas de Software as a Service (SaaS) comum de mercado, desde que não haja risco de dependência tecnológica para disponibilizar esta plataforma.

O cloud broker será o responsável por garantir que os provedores de serviço de nuvem que ele representa:

I - cumpram todos os requisitos previstos nesta norma e na legislação brasileira;

II - operem de acordo com as melhores práticas de segurança.

O PJMA deverá prever no instrumento contratual que o cloud broker poderá ser responsabilizado, civil e administrativamente, por qualquer desconformidade nos provedores que ele representa.

4. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

4.1 Diretoria de Informática e Automação

Compete à Diretoria de Informática e Automação:

I - supervisionar o serviço em nuvem disponibilizado pelo provedor de serviço, observando as disposições desta norma;

II - estabelecer os países nos quais dados e informações custodiados pelo PJMA poderão ser armazenados em soluções de computação em nuvem;

III - definir os requisitos criptográficos mínimos para o armazenamento de dados e informações, custodiados pelo PJMA, em soluções de computação em nuvem;

IV - assegurar a contínua efetividade da comunicação com o provedor de serviço de nuvem, que fornece tais serviços ao PJMA, de forma a assegurar que os controles e os níveis de serviço acordados sejam cumpridos;

V - supervisionar a aplicação de medidas de correção pelo provedor de serviço de nuvem;

VI - comunicar incidentes cibernéticos informados pelo provedor de serviço de nuvem aos órgãos competentes para os seus tratamentos, conforme a relevância dos incidentes previamente estabelecida;

VII - capacitar a equipe responsável por esse gerenciamento nas tecnologias utilizadas pelo provedor de serviço de nuvem;

VIII - exigir que o provedor de serviço de nuvem documente e comunique

seus recursos, papéis e responsabilidades de segurança da informação para o uso de seus serviços;

IX - elaborar uma matriz que inclua obrigações e responsabilidades do PJMA e do provedor de serviço de nuvem;

X - elaborar um processo de tratamento de incidentes junto ao provedor de serviço de nuvem.

5. INFRAÇÕES E PENALIDADES

Infrações e penalidades serão aplicadas conforme previsto na Política de Segurança da Informação.

6. REVISÕES

Esta norma será alterada mediante necessidade de atualização, com apreciação e aprovação do Comitê de Governança de Segurança da Informação (CGSI).

7. APROVAÇÃO

A norma foi aprovada pelo Comitê de Governança de Segurança da Informação (CGSI), revogando-se todas as disposições em contrário.

FRANCISCO SOARES REIS JÚNIOR
Juiz Auxiliar de Entrância Final
Gabinete do Juiz Auxiliar Francisco Soares Reis Júnior

Matrícula 93856

JOSÉ NILO RIBEIRO FILHO
Juiz Auxiliar da Presidência
Gabinete dos Juizes Auxiliares da Presidência
Matrícula 51136

JOSÉ JORGE FIGUEIREDO DOS ANJOS JUNIOR
Diretor da Secretaria da CGJ
Gabinete do Diretor da Secretaria da CGJ
Matrícula 155846

CARLOS ANDERSON DOS SANTOS FERREIRA
Diretor Geral da Secretaria do Tribunal de Justiça
Gabinete do Diretor Geral
Matrícula 193474

CLÁUDIO HENRIQUE CARNEIRO SAMPAIO
Diretor de Informática e Automação
Diretoria de Informática e Automação
Matrícula 99176

LAÉRCIO LEÃO AMARAL
Diretor Judiciário
Diretoria Judiciária
Matrícula 128835

JUREMA MAMEDE DE PAIVA SANTOS
Diretora de Auditoria Interna
Diretoria de Auditoria Interna
Matrícula 107318

MILENA VIEIRA DE OLIVEIRA
Diretora de Recursos Humanos
Diretoria de Recursos Humanos
Matrícula 99671

ANDRE MENEZES MENDES
Diretor do FERJ
Diretoria do FERJ

Matrícula 114819

ISABELLA CAROLINA SILVA E SILVA
Assessora Chefa da Assessoria de Comunicação da Presidência
Assessoria de Comunicação da Presidência
Matrícula 198986

FERNANDO ANTONIO CARVALHO MARQUES
Coordenador de Finanças
Coordenadoria de Finanças
Matrícula 103820

LUIZ GUSTAVO SANTOS NASCIMENTO
Assessor Técnico da Diretoria Administrativa
Diretoria Administrativa
Matrícula 204081

MAYCO MURILO PINHEIRO
Diretor de Engenharia e Arquitetura
Diretoria de Engenharia e Arquitetura
Matrícula 114389

Documento assinado. SÃO LUÍS - ENTRÂNCIA FINAL, 29/08/2023 18:39 (FRANCISCO SOARES REIS JÚNIOR)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 30/08/2023 08:10 (FERNANDO ANTONIO CARVALHO MARQUES)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 30/08/2023 09:09 (JUREMA MAMEDE DE PAIVA SANTOS)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 30/08/2023 09:13 (CARLOS ANDERSON DOS SANTOS FERREIRA)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 30/08/2023 09:54 (ANDRE MENEZES MENDES)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 30/08/2023 10:37 (MILENA VIEIRA DE OLIVEIRA)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 30/08/2023 11:13 (CLÁUDIO HENRIQUE CARNEIRO SAMPAIO)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 30/08/2023 15:57 (MAYCO MURILO PINHEIRO)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 30/08/2023 16:10 (JOSÉ NILO RIBEIRO FILHO)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 31/08/2023 10:15 (ISABELLA CAROLINA SILVA E SILVA)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 31/08/2023 12:12 (LUIZ GUSTAVO SANTOS NASCIMENTO)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 01/09/2023 16:55 (JOSÉ JORGE FIGUEIREDO DOS ANJOS JUNIOR)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 11/09/2023 10:02 (LAÉRCIO LEÃO AMARAL)