ANEXO VIII
NORMA DE CÓPIAS DE SEGURANÇA DA INFORMAÇÃO

Normativos relacionados:

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

Versionamento:

Versão:	2.0
Data:	22/04/2024
Criada por:	Grupo de Trabalho Técnico (GTT) do CGSI
Aprovada por:	Comitê de Governança de Segurança da Informação (CGSI)
Aprovada em:	22/04/2024

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações
12/06/2023	1.0		
22/04/2024	2.0	GTT do CGSI	Conforme arquivo de registro de alterações (changelog).

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 - Glossário 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 Diretoria de Informática e Automação (DIA) não garantirá a realização de cópia de segurança (backup) ou a recuperação de arquivos armazenados localmente nos computadores de mesa (desktop) e notebooks dos(as) usuários(as) ou em quaisquer outros dispositivos fora das áreas de armazenamento disponibilizadas pela DIA, conforme estabelecido no ANEXO VI - Norma de Uso Aceitável de Ativos da PSI.

As cópias de segurança em formato eletrônico pertencentes a ativos e/ou recursos de Tecnologia da Informação e Comunicação (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 serão projetadas para garantir a restauração dos arquivos no menor tempo possível, especialmente em situações de indisponibilidade de ativos e/ou recursos de TIC. Essas rotinas utilizarão soluções próprias e especializadas, automatizando o processo, e possuirão 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 Poder Judiciário do Estado do Maranhão (PJMA).

A infraestrutura de rede para cópias de segurança deverá ser separada, tanto logicamente quanto fisicamente, dos sistemas críticos do PJMA. E, deverá ser garantido reserva de recursos para testes de restauração das informações armazenadas.

A armazenagem das cópias de segurança deverá ser realizada em um local fisicamente separado do ambiente principal de Tecnologia da Informação e Comunicação (TIC). Essa prática possibilita preservar cópias adicionais dos principais serviços e informações que sejam considerados críticos.

Em situações onde a confidencialidade seja considerada importante, é recomendável que as cópias de segurança sejam protegidas por 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 personalizada, a depender de necessidades específicas.

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

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 e personalizada);

IV - tempo de retenção individual, conforme escopo definido;

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

VI - Recovery Time Objective - RTO, que 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 - TJMA ou posterior que a substitua.

5. TIPOS DE CÓPIAS DE SEGURANÇA

O Poder Judiciário do Estado do Maranhão (PJMA) adotará os seguintes tipos de cópias de segurança:

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.

Técnicas de compressão de dados poderão ser utilizadas, desde que o aumento 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). As condições ambientais deverão ser observadas e 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 deverão ser logicamente e 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 deverão ser verificadas periodicamente e seguir 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 03 (três) meses, atendendo aos ambientes de homologação e produção de forma alternada, levando em consideração os recursos de TIC disponíveis.

Os registros de teste de recuperação de cópias de segurança deverão incluir, no mínimo:

I - o tipo de ativo e/ou recurso de TIC, como Máquina Virtual ou Virtual Machine (VM), sistema, serviço ou Banco de Dados, que teve o seu restabelecimento testado;

II - a data da realização do teste;

III - o tempo gasto para finalização do teste (retorno da cópia de segurança);

IV - a situação do procedimento, indicando se foi concluído com sucesso ou se ocorreu alguma falha;

V - uma avaliação se foram atendidos os níveis de serviço pactuados, tais como os Recovery Time Objective – RTOs, considerando os diferentes tipos de ambiente (produção, homologação, etc.) do PJMA e os recursos de TIC disponíveis para cada ambiente.

9. RESTAURAÇÃO DE CÓPIAS 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 estará definido em procedimento interno detalhado da DIA.

A recuperação de mensagens e arquivos eletrônicos da rede corporativa do PJMA e do ambiente colaborativo deverá ser solicitada para a Diretoria de Informática e Automação (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 pelos(as) usuários(as) 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) na rede corporativa do PJMA só será possível se estiverem 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 pelos(as) usuários(as), deverão observar as orientações abaixo:

I - os(as) usuários(as) poderão recuperar, no prazo de 30 (trinta) dias, as mensagens e os arquivos eletrônicos colocados na lixeira;

II - decorridos os 30 (trinta) dias da exclusão ou após a execução do procedimento de “esvaziar a lixeira” realizada pelos(as) usuários(as), o(a) administrador(a) de cópias de segurança terá 25 (vinte e cinco) dias para recuperar as mensagens e/ou os arquivos eletrônicos deletados.

Após o vencimento dos prazos mencionados, as mensagens e arquivos eletrônicos serão automaticamente excluídos pelo serviço do ambiente colaborativo, sem possibilidade de recuperação. Apenas as contas dos magistrados(as) ou das unidades administrativas/judiciais terão a capacidade de restaurar mensagens e arquivos eletrônicos após os prazos informados.

Se uma credencial de acesso ao e-mail for excluída, observando os prazos de bloqueio e exclusão definidos no ANEXO II - Norma de Controle de Acesso e Gestão de Identidade da PSI, o(a) administrador(a) de cópias de segurança poderá recuperar as mensagens e os arquivos eletrônicos dos(as) usuários(as) em até 20 dias a partir da data de exclusão da credencial.

10. DO DESCARTE DA MÍDIA

Para o descarte da mídia da cópia de segurança, dever-se-á:

I - assegurar que a mídia não contenha mais dados ativos 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 (DIA) 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

As 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.