III - acompanhamento regular da evolução das vulnerabilidades técnicas no ambiente da rede corporativa;
IV - comunicação à Comissão de Segurança da Informação (CSI) a respeito da evolução, dos riscos e dos achados dos testes e das varreduras;
V - proposição de melhorias nos processos da gestão de vulnerabilidades para a CSI.
Capítulo VI
DISPOSIÇÕES FINAIS
Art. 13. Os casos omissos serão resolvidos pela CSI.
Art. 14. A revisão desta portaria ocorrerá a cada 3 (três) anos ou sempre que se fizer necessário ou conveniente para o TSE.
Art. 16. O descumprimento desta portaria deve ser imediatamente registrado como incidente de segurança e comunicado à CSI para apuração e consequente adoção das providências cabíveis.
Art. 17. Esta portaria entra em vigor na data de sua publicação e sua implementação se fará no prazo de 12 (doze) meses a contar dessa data.
RUI MOREIRA DE OLIVEIRA
Documento assinado eletronicamente em 20/07/2021, às 14:34, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.
A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1706383&crc=69D9C719, informando, caso não preenchido, o código verificador 1706383 e o código CRC 69D9C719.
2020.00.000004513-0

PORTARIA TSE Nº 457 DE 13 DE JULHO DE 2021.

Institui norma de gerenciamento de *backup* e restauração de dados relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral.
O DIRETOR-GERAL DA SECRETARIA DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições legais e regimentais, considerando a Resolução-CNJ nº 370, de 28 de janeiro de 2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), e a Resolução-TSE nº 23.501, de 19 de dezembro de 2016, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral,
RESOLVE:
Capítulo I
DISPOSIÇÕES PRELIMINARES
Art. 1º Fica instituída a norma de gerenciamento de *backup* e restauração de dados, em consonância com a Política de Segurança da Informação do Tribunal Superior Eleitoral (TSE).
Art. 2º Para os efeitos da Política de Segurança da Informação do TSE, aplicam-se os termos e definições conceituados na Portaria TSE nº 444, de 8 de julho de 2021.
Capítulo II
DO PLANEJAMENTO DA CÓPIA DE SEGURANÇA (*BACKUP*)
Art. 3º As informações do TSE, incluindo dados pessoais, biográficos, biométricos e corporativos, devem ser protegidas por meio de rotinas sistemáticas de cópia de segurança.
Art. 4º A unidade responsável pelo gerenciamento de cópia de segurança, juntamente com os respectivos proprietários dos ativos de informação, deve definir os prazos de realização, retenção e descarte das informações armazenadas na cópia de segurança, respeitando os níveis de classificação atribuídos, de acordo com a necessidade de cada serviço e com as leis que os regulamentem.

Parágrafo único. Ficam estipulados os seguintes prazos máximos de retenção de cópia de segurança:
I - 90 (noventa) dias, como padrão;
II - 2 (dois) anos, como prazo máximo, mediante justificativa fundamentada;
III - acima de 2 (dois) anos, somente em casos de atendimento a previsões legais.
Art. 5º Para execução do disposto no art. 4º, a unidade responsável pelo gerenciamento de cópia de segurança deve definir o correspondente plano de realização, observadas as especificações e a vida útil do sistema de armazenamento.
§ 1º A lista de itens que devem ser contemplados no plano de realização de cópia de segurança incluirá:
I - arquivos de configurações de sistemas operacionais e de seus respectivos servidores da rede corporativa;
II - dados eleitorais e corporativos armazenados em diretórios da rede corporativa;
III - dados eleitorais e corporativos armazenados em banco de dados de produção;
IV - dados dos sistemas de segurança orgânica e acesso às dependências do TSE;
V - mensagens corporativas, como as de correio eletrônico;
VI - principais registros de eventos (*log*) e trilhas de auditoria de sistemas de informação.
§ 2º As cópias de segurança de dados armazenados em banco de dados que não façam parte do ambiente de produção (desenvolvimento, homologação, etc.) deverão ser especificamente solicitadas à unidade responsável pelo gerenciamento de cópia de segurança, acompanhadas de justificativa.
§ 3º A realização de cópias de segurança por ocasião da realização de eleições poderá ser objeto de procedimentos próprios, em razão de especificidades relacionadas aos seus requisitos.
Art. 6º O TSE deverá prover os recursos adequados para a geração e restauração de cópia de segurança, a fim de garantir que as informações críticas sejam recuperadas após incidente, desastre ou falha de mídia de armazenamento.
Art. 7º Caberá à unidade responsável pelo gerenciamento de cópia de segurança documentar e manter atualizadas as rotinas de que cuida este ato normativo quanto às informações armazenadas nos servidores da rede corporativa, considerando, no mínimo, os seguintes elementos:
I - tipo de mídia de armazenamento;
II - requisitos de segurança das informações armazenadas;
III - local de armazenamento das mídias;
IV - período de retenção da cópia de segurança;
V - tipo do *backup*: total (*full*), incremental ou diferencial;
VI - tempo máximo para a restauração da cópia de segurança;
VII - periodicidade da cópia de segurança, a qual poderá ser diária, semanal, mensal ou anual;
VIII - horários permitidos para execução da cópia de segurança;
IX - procedimentos para realização da cópia de segurança;
X - procedimentos e periodicidade de testes de restauração da cópia de segurança;
XI - prazo de suporte do fabricante ao equipamento de cópia de segurança;
XII - procedimentos para descarte e substituição dos equipamentos de cópia de segurança;
XIII - número da revisão ou histórico das versões da documentação;
XIV - identificação do autor ou responsável pela manutenção da documentação.
Art. 8º A documentação do plano e das rotinas de cópia de segurança deve ser armazenada em local seguro e com acesso restrito à seção responsável pelo gerenciamento de cópia de segurança.
Capítulo III

DA REALIZAÇÃO DA CÓPIA DE SEGURANÇA

Art. 9º As tecnologias utilizadas para a realização da cópia de segurança devem cumprir os requisitos necessários para preservar a integridade, a confidencialidade, a disponibilidade e a irretratabilidade das informações, conforme os níveis de classificação atribuídos.

Art. 10. As cópias de segurança devem ser geradas em mídias especificadas pelo fabricante do equipamento da unidade de *backup* e atender ao uso de *hardware* e *software* definidos pela unidade responsável pelo gerenciamento de cópia de segurança.

Art. 11. A cópia de segurança das informações armazenadas nos servidores da rede corporativa deve ser realizada em período de baixa utilização de seus recursos computacionais, preferencialmente fora do horário de expediente ordinário das unidades da Secretaria do Tribunal.

Art. 12. Após a geração da cópia de segurança, devem ser analisados os registros de eventos (*logs*) gerados pela solução de *backup*, para garantir o resultado da operação ou para a adoção de providências cabíveis, nos casos de eventuais erros.

Art. 13. A cópia de segurança em estações de trabalho, *smartphones*, *tablets*, *notebooks* ou outros dispositivos de uso individual é de responsabilidade exclusiva do próprio usuário.

Capítulo IV

DO ARMAZENAMENTO DA CÓPIA DE SEGURANÇA

Art. 14. As informações contidas nas mídias da cópia de segurança devem ser submetidas a mecanismos de segurança para lhes preservar a integridade, a confidencialidade, a disponibilidade e a irretratabilidade, conforme os níveis de classificação atribuídos.

Art. 15. A cópia de segurança, de acordo com sua criticidade, deve ser provida em 2 (duas) mídias distintas, com conteúdo idêntico, para armazenamento em 2 (dois) locais diferentes, observado o seguinte:

I - uma cópia de segurança deve ser armazenada de forma a permitir sua rápida localização e recuperação;

II - outra cópia de segurança deve ser armazenada em local externo à sede do TSE;

III - ao menos uma cópia de segurança deve ser armazenada em uma localização que não seja endereçável de forma contínua por meio de chamadas do sistema operacional.

§ 1º Os locais de armazenamento das mídias da cópia de segurança devem ter mecanismos de segurança, considerando, minimamente, os seguintes elementos:

I - o acesso ao local deve ser restrito e monitorado;

II - o local deve ser protegido contra agentes nocivos naturais (poeira, calor, umidade, entre outros);

III - o local deve ser protegido contra interferências eletromagnéticas;

IV - o local deve possuir controles de prevenção, detecção e combate a incêndio.

§ 2º Os cofres para armazenamento das mídias removíveis da cópia de segurança devem ter mecanismos de segurança, considerando, minimamente, os seguintes elementos:

I - atender à Norma Brasileira ABNT NBR 11515;

II - ter resistência ao fogo, de acordo com a norma BS EN 1047-1;

III - ter resistência ao arrombamento, de acordo com a norma BS EN 14450.

§ 3º Os locais externos de armazenamento da cópia de segurança devem possuir requisitos de segurança adequados e separados do ambiente de armazenagem da cópia principal, de forma que não permaneçam expostos aos mesmos riscos de desastres que a localidade de origem dos dados.

Capítulo V

DA RESTAURAÇÃO DA CÓPIA DE SEGURANÇA

Art. 16. A restauração da cópia de segurança deve ser realizada somente nas seguintes situações:

I - para recompor a integridade do ambiente afetado após um incidente, desastre ou falha de uma mídia de armazenamento;

II - para atender a solicitação formal do proprietário do ativo de informação à unidade responsável pelo gerenciamento de cópia de segurança;
III - para realização de testes de restauração periódicos;
IV - para realização de auditorias e investigações legais e forenses.
Art. 17. A restauração da cópia de segurança de sistemas operacionais e de informações deve ser realizada preferencialmente em máquina isolada do ambiente de produção.
Parágrafo único. Caso o sistema de que trata o *caput* tenha sido comprometido, é obrigatória a revisão de todas as configurações, visando garantir o retorno correto do serviço.
Art. 18. O proprietário do ativo de informação deve validar a integridade das informações restauradas, antes da sua utilização.
Art. 19. Após a restauração da cópia de segurança, devem ser analisados os registros de eventos (*logs*) gerados pela solução de *backup*, para garantir o resultado da operação ou para a adoção de providências cabíveis, no caso de eventuais erros.
Art. 20. Devem ser estabelecidos procedimentos para testes periódicos, por amostragem, de restauração da cópia de segurança, com o intuito de assegurar a integridade dos dados gravados.
Parágrafo único. As informações restauradas devem ser excluídas após a realização dos testes de restauração da cópia de segurança.
Capítulo VI
DO DESCARTE E DA SUBSTITUIÇÃO DA CÓPIA DE SEGURANÇA
Art. 21. O descarte e a substituição da mídia utilizada para geração da cópia de segurança devem respeitar o disposto na Portaria TSE nº 454, de 13 de julho de 2021, que institui a Norma de Controle de Acesso Físico e Lógico relativos à Segurança das Informações e Comunicações do Tribunal Superior Eleitoral.
Art. 22. Nos casos de substituição da solução de *backup* (*hardware* ou *software*), as informações contidas nas mídias da antiga solução devem ser transferidas, em sua totalidade, para mídias compatíveis com a nova solução.
Parágrafo único. A solução de *backup* obsoleta somente poderá ser desativada após a certificação de que todas as informações foram transferidas para a nova solução implementada.
Capítulo VII
DISPOSIÇÕES FINAIS
Art. 23. Cópias de segurança (*backup*) não são consideradas documentos arquivísticos, de forma que permanece a necessidade de que as informações sejam preservadas em sistemas, bases de dados e repositórios arquivísticos digitais confiáveis, nos termos da Portaria-TSE nº 1.013 de 23 de novembro de 2018.
Art. 24. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação (CSI) do TSE.
Art. 25. A revisão desta portaria ocorrerá a cada 3 (três) anos ou sempre que se fizer necessário ou conveniente para o TSE.
Art. 26. O descumprimento desta portaria deve ser imediatamente registrado como incidente de segurança e comunicado à CSI para apuração e consequente adoção das providências cabíveis.
Art. 27. Esta portaria entra em vigor na data de sua publicação e sua implementação se fará no prazo de 12 (doze) meses a contar dessa data.
RUI MOREIRA DE OLIVEIRA
Documento assinado eletronicamente em 20/07/2021, às 14:34, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.
A autenticidade do documento pode ser conferida em

https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1706314&crc=32F25811, informando, caso não preenchido, o código verificador 1706314 e o código CRC 32F25811.
2020.00.000004513-0

ÍNDICE DE ADVOGADOS

ÍNDICE DE PARTES

ÍNDICE DE PROCESSOS