Art. 12. Um sistema de detecção e prevenção de intrusões gerenciado fora do controle dos administradores e operadores da rede corporativa pode ser utilizado para monitorar as atividades nos registros de eventos.

Capítulo V

DA SINCRONIZAÇÃO DOS RELÓGIOS

Art. 13. O horário dos ativos de processamento deve ser ajustado por meio de mecanismos de sincronização de tempo, de forma que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a Hora Legal Brasileira, de acordo com o serviço oferecido e assegurado pelo Observatório Nacional.

Art. 14. O estabelecimento correto dos relógios nos ativos de processamento da rede corporativa é importante para assegurar a exatidão dos registros de eventos, que podem ser requeridos para investigações ou como evidências em casos legais ou disciplinares, devendo atender, no mínimo, às seguintes rotinas:

I - uso de, pelo menos, 3 (três) fontes de tempo sincronizadas, a partir das quais os ativos de processamento recuperem regularmente as informações de data, hora e fuso horário, de forma que os registros de eventos (*logs*) sejam cronologicamente consistentes;

II - preferencialmente, compartilhamento ou sincronização das mesmas fontes de tempo com outros controles de acesso lógico e físico, como catracas, pontos eletrônicos, entre outros, para integrar cronologicamente os sistemas de gerenciamento.

Capítulo VI

DISPOSIÇÕES FINAIS

Art. 15. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação (CSI) do TSE.

Art. 16. A revisão desta portaria ocorrerá a cada 3 (três anos) ou sempre que se fizer necessário ou conveniente para o TSE.

Art. 17. 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. 18. 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=1706379&crc=9BAC2FE1, informando, caso não preenchido, o código verificador 1706379 e o código CRC 9BAC2FE1.

2020.00.000004513-0

PORTARIA TSE Nº 458 DE 13 DE JULHO DE 2021.

Institui norma de gestão de ativos, 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 gestão de ativos, 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 INVENTÁRIO DOS ATIVOS

Art. 3º Todos os ativos de informação e de processamento que utilizem infraestrutura de Tecnologia da Informação, enquanto permanecerem sob responsabilidade ou custódia do TSE, devem ser claramente identificados e inventariados.

Art. 4º O inventário a que se refere o art. 3º deve incluir todos os ativos de informação e de processamento que utilizem a infraestrutura tecnológica do TSE, conectados ou não à rede corporativa, e conter informações indispensáveis:

I - a partir das necessidades de recuperação ou de substituição eficiente dos ativos em caso de desastre;

II - com vistas a atender aos interesses da sociedade e do Estado;

III - para fornecer subsídios aos processos de:

a) Segurança das Infraestruturas Críticas de Informação;

b) Gestão da Segurança da Informação;

c) Gestão de Riscos;

d) Gestão de Continuidade de Negócios;

e) Gerenciamento de Configuração;

f) Gerenciamento de Liberação;

g) Gerenciamento de Problemas;

h) Central de Serviços;

i) Gerenciamento de Mudanças;

j) Gerenciamento de Incidentes;

k) Gestão da Informação e do Conhecimento.

Art. 5º O detalhamento dos ativos deve contemplar, no mínimo, e, quando aplicável, o seguinte conjunto de informações:

I - identificação única (matrícula, número patrimonial, nome, QR Code, RFID, etc.);

II - tipo de ativo;

III - descrição do ativo;

IV - localização;

V - unidade responsável;

VI - proprietário do ativo de informação;

VII - custodiantes;

VIII - informações complementares sobre *software*, como versão, fornecedor, formato, data de instalação, licenças de uso, disponibilidade de suporte, cópia de segurança (*backup*) e aprovação de instalação na rede corporativa;

IX - informações complementares sobre *hardware*, como endereço de Internet Protocol (IP), endereço de *hardware* (MAC Address), nome da máquina e aprovação de conexão à rede corporativa.

Art. 6º Recomenda-se que o detalhamento dos ativos contemple, também, sempre que possível:

I - o levantamento das interfaces e das interdependências internas e externas dos ativos de informação considerados críticos, bem como os impactos quando da indisponibilidade ou destruição de tais ativos de informação, seja no caso de incidentes ou de desastres, visando atender aos interesses da sociedade e do Estado;

II - os requisitos de segurança da informação categorizados, no mínimo, em 5 (cinco) categorias de controle:

a) tratamento da informação;

b) controles de acesso físico e lógico;

c) gestão de risco de segurança da informação;

d) tratamento e respostas a incidentes em redes computacionais;

e) gestão de continuidade dos negócios nos aspectos relacionados à segurança da informação.

Art. 7º O inventário de ativos de TI deve ser único e assegurar compatibilidade e exatidão de conteúdo com outros inventários em uso no TSE, a exemplo do controle patrimonial.

Parágrafo único. As urnas eletrônicas poderão ser controladas em inventário diferenciado, em função de suas especificidades de arquitetura e de utilização.

Art. 8º As informações registradas no inventário de ativos devem ser revisadas em periodicidade não superior a 1 (um) ano e as anomalias encontradas devem ser apresentadas à Comissão de Segurança da Informação (CSI), conforme definições do processo de gerência de configuração.

Capítulo III

DO PROPRIETÁRIO DOS ATIVOS

Art. 9º Cada ativo de informação em uso no TSE deve ter um proprietário formalmente instituído por sua posição ou cargo, responsável primário pela viabilidade e sobrevivência do ativo.

Art. 10. O proprietário do ativo de informação deve assumir, no mínimo, as seguintes responsabilidades:

I - descrição do ativo de informação;

II - definição das exigências de segurança da informação do ativo;

III - comunicação das exigências de segurança da informação do ativo a todos os custodiantes e usuários;

IV - garantia de cumprimento das exigências de segurança da informação, por meio de monitoramento contínuo;

V - indicação dos riscos de segurança da informação que podem afetar os ativos;

VI - garantia da adequada classificação dos ativos sob sua responsabilidade, segundo o grau de segurança das informações nele contidas;

VII - garantia do tratamento adequado, conforme a classificação de segurança das informações nele contidas, de acordo com as orientações descritas na norma de classificação da informação;

VIII - garantia da habilitação de credenciais ou contas de acesso, conforme as restrições ao acesso definidas pelo grau de segurança das informações nele contidas, de acordo com as orientações descritas na norma de classificação da informação;

IX - atualização do inventário quando houver mudança de localização, responsabilidade ou custódia do ativo.

Art. 11. Os proprietários dos ativos de informação devem estabelecer critérios e práticas que assegurem a segregação de funções para que o controle de um processo ou sistema não fique restrito, na sua totalidade, a uma única pessoa, visando à redução do risco de mau uso acidental ou deliberado dos ativos.

Art. 12. O proprietário do ativo de informação poderá delegar as tarefas de rotina para um custodiante, providência que não afastará, todavia, a responsabilidade do primeiro.

Capítulo IV

DA GESTÃO DO INVENTÁRIO DOS ATIVOS

Seção I

CONTROLE DE REDES

Art. 13. Requisitos mínimos de controle devem ser implementados na rede corporativa para assegurar a gestão adequada dos ativos de processamento (*hardwares*) inventariados, entre os quais:

I - utilização de ferramenta de varredura ativa ou passiva para manter automaticamente o inventário atualizado;

II - utilização de ferramentas de gerenciamento de endereço IP para atualizar o inventário;

III - controle sobre quais ativos podem ser conectados à rede corporativa;

IV - garantia de remoção da rede corporativa ou de colocação em quarentena de ativos não autorizados ou de atualização do inventário em tempo hábil.

Art. 14. Requisitos mínimos de controle devem ser implementados na rede corporativa para assegurar a gestão adequada dos ativos de processamento (*softwares*) inventariados:

I - utilização, preferencialmente, de ferramenta de inventário para automatizar o registro de todos os *softwares* utilizados;

II - manutenção de lista atualizada de todos os *softwares* autorizados em uso;

III - garantia de homologação para uso apenas de *software* atualmente suportado pelo fornecedor, cabendo a marcação daquele não suportado no inventário como sem disponibilidade de suporte;

IV - integração dos inventários de *software* e *hardware* para que todos os ativos associados sejam rastreados em um único local;

V - garantia de remoção de *software* não autorizado ou de atualização do inventário em tempo hábil;

VI - avaliação regular dos riscos de uso de *software* física ou logicamente segregado ou isolado da rede corporativa.

Seção II

CONTROLE DE ATIVOS DE PROCESSAMENTO

Art. 15. O processo de gerência de configuração deve assegurar que o inventário dos ativos seja adequadamente gerenciado, atualizado e monitorado em cada fase do ciclo de vida do ativo, quais sejam:

I - aquisição;

II - implementação;

III - manutenção;

IV - descarte.

Capítulo V

DISPOSIÇÕES FINAIS

Art. 16. A Secretaria de Gestão da Informação terá acesso ao inventário de que trata o art. 14 para consulta e emissão de relatório, para fins de atualização do Plano de Classificação das Informações e dos Documentos e da Tabela de Temporalidade dos Documentos, bem como para classificação e avaliação dos ativos de informação do Tribunal.

Art. 17. Os casos omissos serão resolvidos pela CSI.

Art. 18. A revisão desta portaria ocorrerá a cada 3 (três) anos ou sempre que se fizer necessário ou conveniente para o TSE.

Art. 19. 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. 20. 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=1706360&crc=8A3413E4, informando, caso não preenchido, o código verificador 1706360 e o código CRC 8A3413E4.
2020.00.000004513-0

PORTARIA TSE Nº 454 DE 13 DE JULHO DE 2021.

Dispõe sobre a instituição da Norma de Controle de Acesso Físico e Lógico Relativos à Segurança das Informações e Comunicações 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; 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; a Resolução-TSE nº 23.360, de 13 de outubro de 2011, que regulamenta, entre outros, o ingresso de pessoas, objetos e volumes nas dependências do Tribunal; as orientações de controles de segurança da informação dispostas na norma ISO NBR /IEC 27002:2013;a Revisão 1 da Norma Complementar nº 07/IN01/DSIC/GSIPR, homologada em 15 de julho de 2014, que estabelece diretrizes para implantação de controles de acesso relativos à segurança da informação e das comunicações na administração pública federal; e as recomendações do Acórdão-TCU nº 1.603, de 13 de agosto de 2008, item 9.1.3, sobre a importância dos controles de acesso,
RESOLVE:
Art. 1º Fica instituída a Norma de Controle de Acesso Físico e Lógico relativa à segurança das informações e comunicações, em consonância com a Política de Segurança da Informação do Tribunal Superior Eleitoral.
Capítulo I
DOS CONCEITOS E DEFINIÇÕES
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 08 de julho de 2021.
Capítulo II
DOS PRINCÍPIOS
Art. 3º Esta norma tem como princípio norteador a garantia da confidencialidade, integridade e disponibilidade dos ativos de informação.
Art. 4º O acesso, físico ou lógico, deve ser concedido aos usuários deste Tribunal, atendendo aos princípios do perfil de acesso aos ativos de informação.
Capítulo III
DO ESCOPO
Art. 5º O objetivo desta Norma de Controle de Acessos Físico e Lógico Relativos à Segurança das Informações e Comunicações consiste em:
I - estabelecer diretrizes para implantação de controles de acesso físico e lógico;
II - preservar os ativos de informação;
III - assegurar a confidencialidade, integridade e disponibilidade dos ativos de informação sob a responsabilidade deste Tribunal.
Art. 6º Esta portaria se aplica aos magistrados, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiários, prestadores de serviço, colaboradores e usuários externos que utilizam os ativos de informação deste Tribunal.