Tribunal Regional Eleitoral
do Espírito Santo

Sede: Vitória/ES
Av. João Batista Parra, 575
Praia do Suá - Vitória - ES
CEP 72620-000
Tel.: (27) 2121.8595
Endereço eletrônico:
www.tre-es.jus.br

Comissão de Segurança da Informação

NSI-013	V1.0 - JUN 2024	SEGURANÇA DA INFORMAÇÃO

Norma de Gestão de ativos

Referência(s):

Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)

Resolução CNJ 396/2021 – ENSEC-PJ

Resolução TSE 23.644/2021 – PSI/JE

Resolução TSE 23.650/2021 – Política Geral de Privacidade e Proteção de Dados Pessoais

Boas práticas do CIS Controls 8.0

Palavras Chave: segurança, norma, ativos	5 páginas

1. Prefácio

A presente norma está alinhada às diretrizes de Segurança da Informação e dos Dados Pessoais estabelecidas na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) e na Política de Segurança da Informação da Justiça Eleitoral (PSI-JE).

2. Dos conceitos e definições

- **Ferramenta MDM:** As ferramentas do tipo MDM (*Mobile Device Management*) são sistemas projetados para ajudar organizações a gerenciar, monitorar e proteger dispositivos móveis como smartphones, tablets e laptops que estão distribuídos entre funcionários. Essas ferramentas são essenciais em cenários onde os dispositivos precisam ser controlados para garantir a segurança dos dados corporativos e a conformidade com as políticas internas da empresa.

3. Objetivo

Estabelecer diretrizes relativas à gestão de ativos no âmbito do Tribunal Regional Eleitoral do Espírito Santo (TRE-ES).

4. Escopo

4.1. Este normativo se aplica a todos os ativos de informação e processamento sob a responsabilidade ou custódia do TRE/ES e também ativos que não estejam sob controle direto do TRE/ES mas se conectem à rede corporativa regularmente.

4.2. O controle deve abranger ativos conectados à infraestrutura fisicamente, virtualmente, remotamente e aqueles dentro dos ambientes de nuvem.

5. Do inventário de ativos

5.1. Os ativos devem ser claramente identificados e inventariados.

5.2. O inventário deve contemplar no mínimo, e, quando aplicável, o seguinte conjunto de informações:

5.2.1. Identificação única (matrícula, número patrimonial, nome, QR Code, RFID, etc.);

5.2.2. Tipo de ativo;

5.2.3. Descrição do ativo;

5.2.4. Localização;

5.2.5. Unidade responsável;

5.2.6. Proprietário;

5.2.7. Custodiante;

5.3. Para os ativos de hardware, sempre que aplicável, o inventário deve contemplar: o endereço de rede (se estático), endereço de hardware, nome do dispositivo, status de aprovação para conexão à rede.

5.4. Para dispositivos móveis, ferramentas do tipo MDM podem ser utilizadas, quando apropriado.

5.5. Para ativos de software, sempre que aplicável, o inventário deve contemplar: nome do software, editor/criador, data inicial de instalação/uso, versão, status de aprovação para instalação e uso, data de desativação (quanto aplicável).

5.6. Recomenda-se que o inventário descreva para os ativos críticos, sempre que possível, os impactos quando da indisponibilidade ou destruição, seja no caso de incidentes ou de desastres, visando atender aos interesses da sociedade e do Estado.

5.7. As informações registradas no inventário de ativos devem ser revisadas a atualizadas semestralmente.

6. Da Propriedade dos Ativos

6.1. Cada ativo de informação em uso no TRE-ES deve ter um proprietário formalmente instituído por sua posição ou cargo, responsável primário pela viabilidade e sobrevivência do ativo.

6.2. O proprietário do ativo de informação deve assumir, no mínimo, as seguintes responsabilidades, sempre que aplicável:

6.2.1. Garantir que todos os detalhes do ativo sejam registrados corretamente no inventário.

6.2.2. Atualizar imediatamente o inventário de ativos com qualquer alteração relevante, como mudança de localização, transferência de propriedade ou desativação.

6.2.3. Assegurar que o ativo esteja em bom estado de funcionamento e que todas as manutenções necessárias sejam realizadas de forma oportuna.

6.2.4. Implementar e manter medidas de segurança apropriadas para proteger o ativo contra acesso não autorizado, danos, roubo ou perda.

6.2.5. Garantir que o ativo esteja em conformidade com todas as políticas de segurança da informação e normas internas do TRE/ES.

6.2.6. Monitorar o uso do ativo para assegurar que ele seja utilizado apenas para fins autorizados.

6.2.7. Relatar imediatamente qualquer incidente de segurança, mau funcionamento ou uso indevido do ativo à área de TIC ou à Comissão de Segurança da Informação.

6.2.8. Cooperar com auditorias e revisões periódicas de segurança, fornecendo acesso e informações necessárias sobre o ativo.

6.2.9. Garantir que todo software instalado no ativo esteja devidamente licenciado e registrado no inventário de software.

6.2.10. Assegurar que todos os softwares sejam mantidos atualizados com os patches e atualizações mais recentes, conforme orientações da área técnica.

6.2.11. Notificar e atualizar o inventário ao transferir a propriedade ou a responsabilidade do ativo para outro usuário ou setor.

6.2.12. Garantir que a desativação ou descarte do ativo seja realizada de maneira segura, seguindo as diretrizes do TRE/ES para a proteção de dados e a remoção segura de informações.

6.2.13. Participar de treinamentos e capacitações oferecidas pelo TRE/ES relacionados à gestão e segurança de ativos.

6.2.14. Promover e assegurar que todos os usuários do ativo estejam cientes e sigam as melhores práticas de segurança da informação.

6.2.15. 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.

6.3. O proprietário do ativo poderá delegar as tarefas de rotina para um custodiante, providência que não afastará, todavia, a sua responsabilidade.

7. Da gestão do inventário de ativos.

7.1. Ativos de processamento

7.1.1. Utilizar ferramentas de descoberta ativa para identificar todos os ativos conectados à rede do TRE/ES, configurando-a para executar diariamente.

7.1.2. Utilizar ferramentas de descoberta passiva para identificar todos os ativos conectados à rede do TRE/ES, configurando-a para executar semanalmente.

7.1.3. Registrar automaticamente no inventário novos ativos autorizados identificados.

7.1.4. Usar os logs dos servidores DHCP ou ferramentas de gestão de endereço Internet Protocol (IP) para atualizar o inventário de ativos corporativos. Revisar os logs semanalmente visando a atualização dos ativos.

7.1.5. Realizar verificações semanais para identificar ativos não autorizados, removendo-os da rede, negando-lhes o acesso ou colocando-os em quarentena.

7.2. Ativos intangíveis - softwares

7.2.1. Assegurar que apenas softwares atualmente suportados sejam designados como autorizados no inventário e realizar revisão mensal desta condição.

7.2.1.1. Se o software não é suportado, mas é necessário para o cumprimento da missão da empresa, documentar uma exceção detalhando os controles de mitigação e a aceitação do risco residual.

7.2.2. Utilizar ferramentas de inventário de software, quando possível para automatizar descoberta e documentação de software.

7.2.3. Manter controle a fim de garantir que apenas software autorizado possa ser executado e acessado, efetuando revisão semestral.

7.2.4. Manter controle para garantir que apenas bibliotecas de software autorizadas tenham permissão de execução, efetuando revisão semestral.

7.2.5. Manter controles – como assinaturas digitais ou versionamento - para garantir que apenas scripts autorizados tenham permissão de execução, efetuando revisão semestral.

7.2.6. Assegurar que softwares não autorizados sejam retirados de uso, efetuando revisão semestral.

8. Das disposições finais

8.1. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação deste Tribunal.

8.2. A revisão deste normativo ocorrerá sempre que se fizer necessário ou conveniente para este Tribunal, não excedendo o período máximo de 3 (três) anos.

8.3. O descumprimento desta norma será objeto de apuração pela unidade competente do Tribunal e consequente aplicação das penalidades cabíveis a cada caso.

8.4. Esta norma entra em vigor na data de sua aprovação.