TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO

INSTRUÇÃO NORMATIVA Nº 15, DE 30 DE MARÇO DE 2017

Estabelece normas gerais para garantir o Gerenciamento das Operações e Comunicações dos recursos de processamento da informação da Justiça Eleitoral de Pernambuco.

O **PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO**, no uso de suas atribuições, de conformidade com o disposto na Resolução nº 164, de 10 de julho de 2012, e considerando o Plano de Trabalho 2016-2018 da Comissão de Segurança da Informação e o Plano de Trabalho de atendimento à Resolução-CNJ nº 211/2015 – ENTIC-JUD,

RESOLVE:

Art. 1º Os critérios gerais para garantir a operação segura e correta dos recursos de processamento da informação relacionados às atividades essenciais do TRE-PE obedecerão às regras estabelecidas no anexo desta instrução normativa.

Art. 2º As regras estabelecidas nesta instrução normativa deverão ser implantadas gradativamente em até dois anos, a partir de sua publicação.

Art. 3º Esta instrução normativa entra em vigor na data de sua publicação.

Recife, 30 de março de 2016.

Des. ANTÔNIO CARLOS ALVES DA SILVA
Presidente

INSTRUÇÃO NORMATIVA Nº 15/2017

ANEXO

1 - OBJETIVO

Estabelecer critérios gerais para o gerenciamento das operações e comunicações no âmbito das atividades essenciais do TRE-PE.

1.1 - SEÇÕES CONTEMPLADAS NESTA INSTRUÇÃO NORMATIVA

SEÇÃO	NOME	OBJETIVO
S001-1	Procedimentos e Responsabilidades Operacionais	Garantir a operação segura e correta dos recursos de processamento da informação
S001-2	Gerenciamento de Serviços Terceirizados	Implementar e manter o nível apropriado de segurança da informação e de entrega de serviços em linha com acordos de entrega de serviços terceirizados
S001-3	Planejamento e Aceitação dos Sistemas	Minimizar o risco de falhas nos sistemas
S001-4	Proteção contra códigos maliciosos e códigos móveis	Proteger a integridade do software e da informação
S001-5	Cópias de Segurança	Manter a integridade e disponibilidade da informação e dos recursos de processamento de informação
S001-6	Gerenciamento da Segurança em Redes	Garantir a proteção das informações em redes e a proteção da infraestrutura de suporte
S001-7	Manuseio de Mídias	Prevenir contra divulgação ano autorizada, modificação, remoção ou destruição aos ativos, e interrupções das atividades do negócio
S001-8	Trocas de Informações	Manter a segurança na troca de informações e *softwares* internamente à organização e com quaisquer entidades externas
S001-9	Transações via Internet/Intranet	Garantir a segurança de serviços oferecidos via Internet e Intranet, e sua utilização segura
S001-10	Monitoramento	Detectar atividades não autorizadas de processamento da informação

2 - DOCUMENTOS DE REFERÊNCIA

- **NBR/ISO/IEC 27001:2005** –Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da Segurança da Informação - Requisitos
- **NBR/ISO/IEC 27002:2005** - Código de prática para gestão da Segurança da Informação.
- **Decreto 3.505, de 13/06/2000** que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
- **Política de Gestão e Segurança da Informação** que institui a Política de Segurança da Informação no âmbito da Justiça Eleitoral.

3 - DEFINIÇÕES

- **Afastamento Temporário:** afastamento por qualquer período, com previsão de retorno ao trabalho.
- **Chefia imediata:** servidor da Justiça Eleitoral que exerce a atividade hierárquica imediatamente superior ao servidor em questão.
- **Contas de administração de domínios**: contas especiais utilizadas para administração dos domínios da rede. Conta de administração da rede.
- **Contas de administração de servidores:** contas especiais utilizadas para administração dos servidores.
- **Contas de visita:** contas especiais destinadas a acessos pontuais, como por exemplo *guest*.
- **Contas especiais:** contas padrão do sistema de informação, contas de serviço e contas para administração de recursos de informação.
- **Rede:** Rede Corporativa.
- **Servidores**: profissionais integrantes do quadro de lotação da Justiça Eleitoral

- **Equipamentos de conectividade:** equipamentos responsáveis pela conectividade na infraestrutura de rede, como por exemplo, *switches*, roteadores, *hubs*, *modems* etc.
- **Equipamentos de rede:** servidores, equipamentos de conectividade e estações de gerenciamento.
- **Identificação da conta:** *login* do usuário, *username*.
- **Prestadores de Serviço:** colaboradores que pertencem a outras empresas e realizam trabalhos para a Justiça Eleitoral.
- **Usuários:** pessoas que acessam ou fazem uso de recursos ou sistemas de informação da Justiça Eleitoral.
- **Código móvel:** código transferido de um computador a outro executando automaticamente e realizando funções específicas com pequena ou nenhuma interação por parte do usuário.

4 - SEÇÃO S001-1: PROCEDIMENTOS E RESPONSABILIDADES OPERACIONAIS

Objetiva garantir a operação segura e correta dos recursos de processamento da informação

4.1 - Documentação dos procedimentos de operação

4.1.1 - Os procedimentos de operação devem ser documentados, mantidos atualizados e disponíveis a todos os usuários que deles necessitem.

4.1.2 - Devem ser documentados procedimentos para as atividades de sistemas associadas a recursos de processamento e comunicação de informações, tais como:

4.1.2.1 - inicialização e desligamento de computadores;

4.1.2.2 - geração de cópias de segurança (*backup*);

4.1.2.3 - manutenção de equipamentos;

4.1.2.4 - tratamento de mídias.

4.1.3 - Os procedimentos de operação devem especificar as instruções para a execução detalhada de cada tarefa, incluindo, sempre que aplicável:

4.1.3.1 - processamento e tratamento da informação;

4.1.3.2 - *backup*;

4.1.3.3 - requisitos de agendamento, incluindo interdependência com outros sistemas;

4.1.3.4 - instruções para tratamento de erros ou outras condições excepcionais;

4.1.3.5 - dados para contatos de suporte no caso de eventos operacionais inesperados ou dificuldades técnicas;

4.1.3.6 - instruções especiais quanto ao manuseio e saída de mídias, com uso de formulários específicos;

4.1.3.7 - procedimentos para o reinício e recuperação em caso de falha do sistema;

4.1.3.8 - gerenciamento de trilhas de auditoria e informações de registros (*logs*) de sistemas.

4.2 - Gestão de mudanças

4.2.1 - Modificações nos recursos de processamento da informação e sistemas devem ser controladas.

4.2.2 - O controle de gestão de mudanças deve considerar:

4.2.2.1 - identificação e registro das mudanças significativas;

4.2.2.2 - planejamento e testes das mudanças;

4.2.2.3 - avaliação de impactos potenciais, incluindo impactos de segurança;

4.2.2.4 - procedimento formal de aprovação das mudanças propostas;

4.2.2.5 - comunicação dos detalhes das mudanças para todas as pessoas envolvidas;

4.2.2.6 - procedimentos de recuperação, incluindo procedimentos e responsabilidades pela interrupção e recuperação de mudanças em caso de insucesso ou na ocorrência de eventos inesperados.

4.2.3 - O controle de gestão de cada mudança deve ser conduzido pela área solicitante da mudança, submetida formalmente ao Comitê Executivo da respectiva unidade.

4.3 - Segregação de funções

4.3.1 - Funções e áreas de responsabilidade devem ser segregadas para reduzir as oportunidades de modificação ou uso indevido não autorizado ou não intencional dos ativos da organização.

4.4 - Separação dos ambientes de desenvolvimento, teste e de produção

4.4.1 - Ambientes de desenvolvimento, teste e produção devem ser separados para reduzir o risco de acessos ou modificações não autorizadas aos sistemas operacionais

4.4.2 - Para separação dos ambientes de produção, testes e desenvolvimento devem ser considerados:

4.4.2.1 - regras definidas e documentadas para a transferência de *software* da situação de desenvolvimento para a de produção;

4.4.2.2 - compiladores, editores e outras ferramentas de desenvolvimento ou utilitários de sistemas não acessíveis a partir de sistemas operacionais, quando não for necessário;

4.4.2.3 - ambientes de testes que emulem o ambiente de produção o mais próximo possível;

4.4.2.4 - usuários com diferentes perfis para sistemas em testes e em produção, e que os menus mostrem mensagens apropriadas de identificação para reduzir riscos de erro;

4.4.2.5 - dados sensíveis não disponíveis para os ambientes de testes.

5 - SEÇÃO S001-2: GERENCIAMENTO DE SERVIÇOS TERCEIRIZADOS

Objetiva implementar e manter o nível apropriado de segurança da informação e de entrega de serviços em consonância com acordos de entrega de serviços terceirizados.

5.1 - Entrega de serviços

5.1.1 - Deve ser garantido que os controles de segurança, as definições de serviço e os níveis de entrega de serviços terceirizados sejam implementados, executados e mantidos pelo terceiro.

5.1.2 - O contratante deve garantir que o terceiro mantenha capacidade de serviço suficiente, juntamente com planos de operação viáveis projetados para proporcionar os níveis de continuidade de serviços acordados.

5.2 - Monitoramento e análise crítica de serviços terceirizados

5.2.1 - Os serviços, relatórios e registros providos pelo terceiro devem ser regularmente monitorados e analisados criticamente.

5.3 - Gerenciamento de mudanças para serviços terceirizados

5.3.1 - Mudanças no fornecimento dos serviços, incluindo manutenção e melhoria da política de segurança da informação, dos procedimentos e controles existentes, devem ser gerenciadas, levando-se em conta a criticidade dos sistemas e processos de negócio envolvidos e a reavaliação de riscos.

6 - SEÇÃO S001-3: PLANEJAMENTO E ACEITAÇÃO DOS SISTEMAS

Objetiva minimizar o risco de falhas nos sistemas.

6.1 - Gestão de capacidade

6.1.1 - A utilização dos recursos deve ser monitorada e ajustada, e as projeções feitas para garantir a disponibilidade adequada de capacidade futura, para entrega do desempenho desejado ao sistema.

6.1.2 - Requisitos de capacidade devem ser identificados para cada atividade nova ou em andamento.

6.1.3 - Ajustes e monitoramento dos sistemas devem ser aplicados para melhorar a disponibilidade e eficiência dos sistemas.

6.1.4 - Controles de detecção devem ser implantados para identificar problemas em tempo hábil, sempre que possível.

6.1.5 - Projeções de capacidade futura devem considerar os requisitos de novos negócios e sistemas e as tendências atuais e projetadas de capacidade de processamento de informação.

6.1.6 - Informações provenientes do monitoramento da capacidade devem ser utilizadas para identificar e evitar os potenciais gargalos e a dependência em pessoas-chave que possam representar ameaças à segurança dos sistemas ou aos serviços, e devem orientar o planejamento de ação corretiva apropriada.

6.2 - Aceitação de sistemas

6.2.1 - Devem ser estabelecidos critérios de aceitação para novos sistemas, inclusive sistemas operacionais, atualizações e novas versões e que sejam efetuados testes apropriados do(s) sistema(s) durante seu desenvolvimento, quando couber, e antes da sua aceitação.

6.2.2 - Devem ser considerados os seguintes itens para aceitação formal, sempre que possível:

6.2.2.1 - requisitos de desempenho e de capacidade computacional;

6.2.2.2 - recuperação de erros, procedimentos de reinicialização e planos de contingência;

6.2.2.3 - preparação e teste de procedimentos operacionais de rotina;

6.2.2.4 - concordância do titular da unidade gestora sobre o conjunto de controles de segurança utilizados;

6.2.2.5 - procedimentos manuais eficazes;

6.2.2.6 - requisitos de continuidade dos negócios;

6.2.2.7 - evidência de que a instalação do novo sistema não afetará de forma adversa os sistemas existentes, particularmente nos períodos de pico de processamento;

6.2.2.8 - evidência de que tenha sido considerado o impacto do novo sistema na segurança;

6.2.2.9 - treinamento na operação ou uso de novos sistemas;

6.2.2.10 - facilidade de uso, uma vez que afeta o desempenho do usuário e evita falhas humanas.

7 - SEÇÃO S001-4: PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS E CÓDIGOS MÓVEIS

Objetiva proteger a integridade do *software* e da informação.

7.1 - Controle contra códigos maliciosos

7.1.1 - Devem ser implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.

7.1.2 - Para a proteção contra códigos maliciosos devem ser considerados:

7.1.2.1 - proibição de uso de *softwares* não autorizados pela área de TIC;

7.1.2.2 - análises críticas regulares dos *softwares* e dados dos sistemas que suportam processos críticos (essenciais) de negócio;

7.1.2.3 - investigação formal quando da identificação da presença de quaisquer arquivos não aprovados ou atualização não autorizada;

7.1.2.4 - instalação e atualização regulares de *softwares* de detecção e remoção de códigos maliciosos para o exame de computadores e mídias digitais, de forma preventiva e de forma rotineira;

7.1.2.5 - implementação de procedimentos regulares para coletar informações, tais como assinaturas de listas de discussão e visitas a *sites* informativos sobre novos códigos maliciosos.

7.2 - Controles contra códigos móveis

7.2.1 - Onde o uso de códigos móveis é autorizado, a configuração deve garantir que o código móvel autorizado opere de acordo com uma política de segurança da informação claramente definida, e códigos móveis não autorizados tenham sua execução impedida.

7.2.2 - Para a proteção contra códigos móveis não autorizados devem ser considerados:

7.2.2.1 - execução de códigos móveis em ambientes isolados logicamente;

7.2.2.2 - bloqueio de qualquer tipo de código móvel;

7.2.2.3 - bloqueio do recebimento de códigos móveis;

7.2.2.4 - ativação de medidas técnicas para garantir que o código móvel esteja sendo administrado;

7.2.2.5 - controle dos recursos disponíveis para acesso ao código móvel;

7.2.2.6 - controles criptográficos de autenticação exclusiva do código móvel, quando existente.

8 - SEÇÃO S001-5: CÓPIAS DE SEGURANÇA

Objetiva manter a integridade e disponibilidade da informação e dos recursos de processamento de informação.

8.1 - Cópias de segurança das informações

8.1.1 - Cópias de segurança das informações e dos *softwares* devem ser efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.

8.1.2 - Os seguintes itens devem ser considerados:

8.1.2.1 - produção de registros completos e exatos das cópias de segurança e documentação apropriada os procedimentos de restauração;

8.1.2.2 - definição do nível necessário das cópias de segurança das informações;

8.1.2.3 - extensão e frequência da geração das cópias de segurança em sintonia com os requisitos de negócio e a criticidade da informação para a continuidade da operação do órgão;

8.1.2.4 - armazenamento das cópias de segurança em local distante o suficiente para escapar dos danos de um desastre ocorrido no local principal;

8.1.2.5 - nível apropriado de proteção física e ambiental das informações das cópias de segurança, consistentes com as regras aplicadas na instalação principal;

8.1.2.6 - controles aplicados às mídias na instalação principal aplicados no local das cópias de segurança;

8.1.2.7 - testes regulares das mídias de cópias de segurança para garantir que são suficientemente confiáveis para uso de emergência, se necessário;

8.1.2.8 - procedimentos de recuperação sejam verificados e testados regularmente;

8.1.2.9 - em situações de confidencialidade e quando solicitado formalmente à unidade responsável, as cópias de segurança sejam protegidas por encriptação.

9 - SEÇÃO S001-6: GERENCIAMENTO DA SEGURANÇA EM REDES

Objetiva garantir a proteção das informações em redes e a proteção da infraestrutura de suporte.

9.1 - Controles de redes

9.1.1 - Redes devem ser adequadamente gerenciadas e controladas, de forma a protegê-las contra ameaças e manter a segurança de sistemas e aplicações que utilizam estas redes, incluindo a informação em trânsito.

9.2 - Segurança dos serviços de rede

9.2.1 - Características de segurança, níveis de serviço e requisitos de gerenciamento dos serviços de rede devem ser identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente ou terceirizados.

9.2.2 - Serviços de rede incluem o fornecimento de conexões, serviços de rede privados, redes de valor agregado e soluções de segurança de rede gerenciadas como *firewalls* e sistemas de detecção de intrusos.

10 - SEÇÃO S001-7: MANUSEIO DE MÍDIAS

Objetiva prevenir contra divulgação não autorizada, modificação, remoção ou destruição aos ativos, e interrupções das atividades do negócio.

10.1 - Gerenciamento de mídias removíveis

10.1.1 - Devem existir procedimentos implementados para o gerenciamento de mídias removíveis.

10.1.2 - Mídia removível inclui fitas, discos, *flash disks*, discos removíveis, CD, DVD e mídia impressa.

10.1.3 - Devem ser consideradas as seguintes diretrizes:

10.1.3.1 - o conteúdo de qualquer meio digital reutilizável deve ser destruído, caso venha a ser retirado do órgão;

10.1.3.2 - a remoção de qualquer mídia do órgão deve ser requerida formalmente à chefia imediata;

10.1.3.3 - as mídias devem ser guardadas de forma segura em um ambiente protegido, de acordo com as especificações do fabricante;

10.1.3.4 - informações armazenadas em mídias que precisam estar disponíveis por muito tempo devem também ser armazenadas em outro local para evitar perda;

10.1.3.5 - unidades de mídias removíveis devem ser habilitadas somente se houver uma necessidade do negócio.

10.2 - Descarte de mídias

10.2.1 - As mídias devem ser descartadas de forma segura e protegidas quando não forem mais necessárias, por meio de procedimentos formais.

10.2.2 - O descarte seguro de mídias contendo informações sensíveis deve ser através de incineração ou trituração, ou outro meio que venha a substituí-los e oferte o mesmo resultado e segurança.

10.3 - Procedimentos para tratamento de informação

10.3.1 - Devem ser estabelecidos procedimentos para o tratamento e o armazenamento de informações, para protegê-las contra divulgação não autorizada; mau uso ou uso indevido.

10.3.2 - O tratamento, processamento, armazenamento e transmissão da informação devem ser realizados de acordo com a sua classificação.

10.4 - Segurança da documentação dos sistemas

10.4.1 - A documentação dos sistemas deve ser protegida contra acessos não autorizados.

10.4.2 - Devem ser consideradas as seguintes diretrizes:

10.4.2.1 - a documentação dos sistemas deve ser guardada de forma segura;

10.4.2.2 - a relação de pessoas com acesso autorizado à documentação de sistemas seja a menor possível;

10.4.2.3 - a documentação de sistema mantida em uma rede pública, ou fornecida através de uma rede pública seja protegida de forma apropriada.

11 - SEÇÃO S001-8: TROCA DE INFORMAÇÕES

Objetiva manter a segurança na troca de informações e *softwares* internamente ao órgão e com quaisquer entidades externas.

11.1 - Políticas e procedimentos para troca de informações

11.1.1 - Políticas, procedimentos e controles devem ser estabelecidos e formalizados para proteger a troca de informações em todos os tipos de recursos de comunicação.

11.1.2 - Devem ser considerados os seguintes tópicos:

11.1.2.1 - adoção de procedimentos para proteger a informação em trânsito contra interceptação, cópia, modificação, desvio e destruição;

11.1.2.2 - uso de procedimentos para detecção e proteção contra código malicioso que pode ser transmitido através do uso eletrônico de comunicação;

11.1.2.3 - adoção de procedimentos de proteção de informações eletrônicas sensíveis que sejam transmitidas na forma de anexos;

11.1.2.4 - uso de técnicas de criptografia para proteger a confidencialidade, a integridade e a autenticidade das informações;

11.1.2.5 - informações críticas ou sensíveis não devem ser deixadas em equipamentos de impressão;

11.1.2.6 - adoção de precauções adequadas para evitar que conversas telefônicas confidenciais sejam escutadas ou interceptadas;

11.1.2.7 - uso de dispositivos móveis do TRE-PE (funcionais) exclusivamente para atendimento às necessidades do trabalho;

11.1.2.8 - uso exclusivo de redes sociais em dispositivos ou linhas telefônicas funcionais para atendimento às necessidades do negócio;

11.1.2.9 - exclusão de mensagens contendo informações sensíveis veiculadas através de dispositivos móveis e redes sociais.

11.2 - Acordos para a troca de informações

11.2.1 - Devem ser estabelecidos acordos para a troca de informações e *softwares* entre a organização e entidades externas.

11.3 - Correio Eletrônico

11.3.1 - As informações que trafegam em mensagens eletrônicas devem ser adequadamente protegidas.

11.3.2 - Devem ser consideradas as seguintes diretrizes para a segurança da informação em mensagens eletrônicas:

11.3.2.1 - proteção das mensagens contra acesso não autorizado, modificação ou negação do serviço;

11.3.2.2 - adoção de cuidados para o endereçamento correto da mensagem;

11.3.2.3 - confidencialidade e disponibilidade geral do serviço.

11.4 - Sistemas de informações do negócio

11.4.1 - Políticas e procedimentos devem ser desenvolvidos e implementados para proteger as informações, associadas com a interconexão de sistemas de informações do negócio.

12 - SEÇÃO S001-9: TRANSAÇÕES VIA INTERNET/INTRANET

Objetiva garantir a segurança de serviços oferecidos via Internet e Intranet, e sua utilização segura.

12.1 - Transações *On-Line*

12.1.1 - Informações envolvidas em transações *on-line* institucionais devem ser protegidas para prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada.

12.1.2 - Devem ser considerados os seguintes itens:

12.1.2.1 - uso de assinaturas eletrônicas para transações *on-line* críticas;

12.1.2.2 - para todos os aspectos da transação sejam garantidos credenciais válidas e verificáveis; confidencialidade, integridade, protocolos de comunicação seguros e armazenamento dos detalhes da transação em local fora de qualquer ambiente publicamente acessível.

12.2 - Informações publicamente disponíveis

12.2.1 - A integridade das informações disponibilizadas em sistemas publicamente acessíveis deve ser protegida para prevenir modificações não autorizadas.

12.2.2 - Sistemas de publicação eletrônica, especialmente que permitem realimentação e entrada direta de informação, devem ser cuidadosamente controlados, de forma que:

12.2.2.1 - informações sejam obtidas em conformidade com legislação de proteção de dados;

12.2.2.2 - informações que sejam entradas sejam processadas completa e corretamente em um tempo adequado;

12.2.2.3 - informações sensíveis sejam protegidas durante a coleta, processamento e armazenamento;

12.2.2.4 - não haja acesso intencional ou não a redes às quais o sistema está conectado.

13 - SEÇÃO S001-10: MONITORAMENTO

Objetiva detectar atividades não autorizadas de processamento da informação.

13.1 - Registros de auditoria

13.1.1 - Registros *(log)* de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação devem ser produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso.

13.1.2 - Os registros *(logs)* devem incluir, quando relevante:

13.1.2.1 - identificação do usuário;

13.1.2.2 - datas, horários e detalhes de eventos-chave, tais como horário de entrada *(log-on)* e saída *(log-off)* no sistema;

13.1.2.3 - identidade do terminal ou, quando possível, a sua localização;

13.1.2.4 - registros das tentativas de acesso ao sistema aceitas e rejeitadas;

13.1.2.5 - registro das tentativas de acesso a outros recursos e dados aceitos e rejeitados;

13.1.2.6 - alterações na configuração do sistema;

13.1.2.7 - uso de privilégios;

13.1.2.8 - uso de aplicações e utilitários do sistema;

13.1.2.9 - arquivos acessados e tipo de acesso;

13.1.2.10 - endereços e protocolos de rede;

13.1.2.11 - alarmes provocados pelo sistema de controle de acesso;

13.1.2.12 - ativação e desativação dos sistemas de proteção, tais como sistemas antivírus e sistemas de detecção de intrusos.

13.2 - Monitoramento do uso do sistema

13.2.1 - Devem ser estabelecidos procedimentos para o monitoramento do uso dos recursos de processamento da informação e os resultados das atividades de monitoramento devem ser analisados criticamente de forma regular.

13.3 - Proteção das informações dos registros (*logs*)

13.3.1 - Os recursos e informações de registros *(log)* devem ser protegidos contra falsificação e acesso não autorizado.

13.4 - Registros (*log*) de Administrador e Operador

13.4.1 - As atividades dos administradores e operadores do sistema devem ser registradas

13.5 - Registros (*logs*) de falhas

13.5.1 - As falhas ocorridas devem ser registradas e analisadas, e devem ser adotadas as ações apropriadas.

13.6 - Sincronização dos relógios

13.6.1 - Os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, devem ser sincronizados de acordo com uma hora oficial.