TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO

INSTRUÇÃO NORMATIVA Nº 16, DE 30 DE MARÇO DE 2017

Estabelece normas gerais para garantir a Gestão de Incidentes de Segurança 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 notificação de fragilidades e eventos de segurança da informação no âmbito das atividades essenciais do TRE-PE obedecerá às regras estabelecidas no anexo desta instrução normativa.

Art. 2º As regras estabelecidas nesta instrução normativa devem ser implantadas gradativamente em até 180 dias, 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 16/2017

ANEXO

1 - OBJETIVO

Estabelecer critérios gerais para notificação de fragilidades e eventos de segurança da informação no âmbito das atividades essenciais do TRE-PE.

1.1 - SEÇÕES CONTEMPLADAS NESTA INSTRUÇÃO NORMATIVA

SEÇÃO	NOME	OBJETIVO
S001-1	Notificação de fragilidades e eventos de segurança da informação	Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.
S001-2	Gestão de incidentes de segurança da informação e melhorias	Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança 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 do TRE-PE 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 do TRE-PE.
- **Equipamentos de conectividade:** equipamentos responsáveis pela conectividade na infraestrutura de rede, como por exemplo, *switches*, roteadores, *hubs*, *modens* 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 o TRE-PE.
- **Usuários:** pessoas que acessam ou fazem uso de recursos ou sistemas de informação do TRE-PE.

4 - SEÇÃO S001-1: NOTIFICAÇÃO DE FRAGILIDADES E EVENTOS DE SEGURANÇA DA INFORMAÇÃO

Objetiva assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.

4.1 - Notificação de eventos de segurança da informação

4.1.1 - São exemplos de eventos e incidentes de segurança da informação:

4.1.1.1 - perda de serviço, equipamento ou recursos;

4.1.1.2 - mau funcionamento ou sobrecarga de sistema;

4.1.1.3 - erros humanos;

4.1.1.4 - não conformidade com políticas e diretrizes;

4.1.1.5 - violações de procedimentos de segurança física;

4.1.1.6 - mudanças descontroladas de sistemas, tais como realizadas sem monitoramento ou em decorrência de invasão.

4.1.1.7 - mau funcionamento de *software* ou *hardware*

4.1.1.8 - violação de acesso.

4.1.2 - Os eventos de segurança da informação devem ser relatados para as áreas responsáveis assim que forem observados.

4.1.3 - O relato deve conter detalhes importantes, tais como tipo de não conformidade, violação, mau funcionamento, mensagem na tela, comportamento estranho.

4.1.4 - O usuário não deverá realizar nenhuma ação própria, e sob nenhuma circunstância, tentar averiguar uma fragilidade do item suspeito (*link*, funcionalidade do sistema ou qualquer outro item informacional), para evitar o risco de causar danos ao sistema ou serviço de informação. O descumprimento dessa orientação pode resultar em responsabilidade legal.

4.2 - Notificando fragilidades de segurança da informação

4.2.1 - Os servidores, fornecedores e prestadores de serviços devem ser instruídos a registrar e notificar qualquer observação ou suspeita de fragilidade em sistemas ou serviços.

4.2.2 - As notificações de fragilidade de segurança da informação devem ser encaminhadas através de formulário próprio ao Gestor do Ativo (Instrução Normativa TRE-PE nº 11/2016) e a Comissão de Segurança da Informação.

4.2.3 - O formulário para notificação de fragilidade de segurança da informação deve estar disponível na intranet.

5 - SEÇÃO S001-2: GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E MELHORIAS

Objetiva assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação.

5.1 - Responsabilidades e procedimentos

5.1.1 - Devem ser mantidos *logs* em meio digital, contendo as informações referentes a eventos de segurança da informação por um período a ser definido pelo gestor do ativo definido como crítico pela alta gestão do TRE-PE:

5.1.1.1 - análise de problemas internos;

5.1.1.2 - uso como evidência forense para o caso de uma potencial violação de contrato ou de normas reguladoras ou em caso de delitos civis ou criminais;

5.1.1.3 - negociação para compensação ou ressarcimento por parte de fornecedores.

5.1.2 - Devem ser realizadas rotinas diárias de cópias de segurança, que ficarão armazenadas por um período mínimo definido pelo gestor de cada ativo definido como crítico pela alta gestão do TRE-PE.

5.1.3 - Devem ser adotados mecanismos de detecção de:

5.1.3.1 - códigos maliciosos;

5.1.3.2 - *denial of service* (negação de serviço);

5.1.3.3 - violações de confidencialidade e integridade;

5.1.3.4 - uso impróprio de sistemas de informação.

5.1.4 - Da análise e identificação da causa do incidente deve(m) ser:

5.1.4.1 - implementada(s) ação(ões) corretiva(s) para prevenir a sua repetição.

5.1.4.2 - comunicada aos usuários afetados ou envolvidos a recuperação do incidente.

5.1.4.3 - registrados na Base de Conhecimento (Instrução Normativa TRE-PE nº 7/2015) os eventos e incidentes e os procedimentos adotados.

5.1.5 - As ações para recuperação de violações de segurança e correção de falhas devem ser:

5.1.5.1 - realizadas por servidores/prestadores de serviços explicitamente identificados e autorizados;

5.1.5.2 - documentadas em detalhe;

5.1.5.3 - analisadas criticamente de maneira ordenada e relatadas para Comissão de Segurança da Informação.

5.2 - Aprendendo com os incidentes de segurança da informação

5.2.1 - Devem ser estabelecidos mecanismos para permitir que tipos, quantidades e custos dos incidentes de segurança da informação sejam quantificados e monitorados.

5.2.2 - Devem ser realizadas análises semestrais de incidentes de segurança da informação para identificar eventos recorrentes ou de alto impacto, que podem indicar a necessidade de melhorias ou controles adicionais para limitar a frequência, os danos e os custos.

5.2.3 - As análises de incidentes de segurança da informação devem ser consideradas quando das revisões da política de segurança da informação.

5.3 - Coleta de evidências

5.3.1 - Nos casos em que uma ação de acompanhamento contra uma pessoa ou organização, após um incidente de segurança da informação, envolver uma ação legal (civil ou criminal), evidências devem ser coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento de evidências da jurisdição ou jurisdições pertinentes.