ATO ADMINISTRATIVO Nº 031/2024/EVERESTE

Aprova o Protocolo de Investigação de Ilícitos Cibernéticos no âmbito do Instituto de Tecnologia e Inovação Evereste.

O **Presidente do INSTITUTO DE TECNOLOGIA E INOVAÇÃO EVERESTE** – associação civil de direito privado, sem fins lucrativos, de duração indeterminada – André Fabiano Santos Pereira, no uso de suas atribuições legais e estatutárias, e

CONSIDERANDO o disposto nos termos do Art. 39 do Estatuto Social;

CONSIDERANDO a Lei no 13.709/2018 – Lei Geral de Proteção de Dados; a Lei n° 12.965/2014 – Marco Civil da Internet; o Decreto no 8.771/2016, e a Lei n° 12.527/2011 – Lei de Acesso à Informação;

CONSIDERANDO Norma ABNT NBR ISO/IEC 27002:2013, que normatiza o Código de Prática para Controles da Segurança da Informação;

CONSIDERANDO Promover adequação e alinhamento às regulamentações, normas e melhores práticas relacionadas à segurança cibernética.

RESOLVE:

Art. 1º - APROVAR o **PROTOCOLO DE INVESTIGAÇÃO DE ILÍCITOS CIBERNÉTICOS** na forma do anexo único deste Ato, no âmbito do Instituto de Tecnologia e Inovação Evereste.

Art. 2º - Este Ato entra em vigor na data de sua publicação.

Manaus, 23 de fevereiro de 2024.

ANDRE FABIANO SANTOS PEREIRA:77147715349

Assinado de forma digital por ANDRE FABIANO SANTOS PEREIRA:77147715349
Dados: 2024.02.26 11:42:45 -04'00'

ANDRÉ FABIANO SANTOS PEREIRA

Presidente do Evereste

EVERESTE
INSTITUTO DE TECNOLOGIA E INOVAÇÃO

PROTOCOLO DE

INVESTIGAÇÃO DE ILÍCITOS CIBERNÉTICOS

MANAUS
2024

SUMÁRIO

CAPÍTULO I

DO OBJETIVO

Art. 1° O objetivo do protocolo de investigação de ilícitos cibernéticos é estabelecer diretrizes e procedimentos para investigar crimes cometidos no ambiente virtual. Esse protocolo tem como objetivo principal identificar, coletar e preservar evidências digitais, bem como rastrear e responsabilizar os autores desses crimes, visando garantir a eficácia e a legalidade das investigações, além de contribuir para a segurança cibernética e o combate à criminalidade online.

CAPÍTULO II

DAS DEFINIÇÕES

Art. 2° Para efeito desta portaria, são estabelecidos os seguintes conceitos e definições:

I – Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação;

II – Aquisição de evidência: processo de coleta e cópia das evidências de incidente de segurança em redes computacionais;

III – Ativos de informação: os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso;

IV – Auditoria: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas à consecução dos objetivos;

V – Autenticação: processo de identificação das partes envolvidas em um processo;

VI – Autenticidade: propriedade indicativa de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

VII – Autorização: processo que visa garantir que as informações são acessíveis exclusivamente àqueles com permissão de acesso;

VIII – Coleta de evidências de segurança em redes computacionais: processo de obtenção de itens físicos que contém uma potencial evidência, mediante a utilização de metodologia e ferramentas adequadas. Esse processo inclui a aquisição, ou seja, a geração das cópias das mídias, ou coleção de dados que contenham evidências do incidente;

IX – Endereço IP (Internet Protocol): refere-se ao conjunto de elementos numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores;

X – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

XI – Evidência digital: informação ou dado, armazenado ou transmitido eletronicamente, em modo binário, que pode ser reconhecida como parte de um evento;

XII – Incidente de segurança em redes computacionais: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XIII – Informação sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

XIV – Log ou registro de auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional.

XV – Metadados: conjunto de dados estruturados que descrevem informação primária;

XVI – Preservação de evidência de incidentes em redes computacionais: é o processo que compreende a salvaguarda das evidências e dos dispositivos, de

modo a garantir que os dados ou metadados não sofram alteração, preservando-se a integridade e a confidencialidade das informações;

CAPÍTULO III

DA ADEQUAÇÃO DOS ATIVOS TECNOLÓGICOS

Art. 3° O horário dos ativos de informação deve ser ajustado por meio de mecanismos de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a “Hora Legal Brasileira (HLB)”, de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON).

Art. 4° Os ativos de informação devem ser configurados de forma a registrar todos os eventos relevantes de Segurança da Informação e Comunicação, tais como:

I – autenticação, tanto as bem-sucedidas quanto as malsucedidas;

II – acesso a recursos e dados privilegiados; e

III – acesso e alteração nos registros de auditoria.

Art. 5° Os registros dos eventos previstos no artigo anterior devem incluir as seguintes informações:

I - identificação inequívoca do usuário que acessou o recurso;

II - natureza do evento, como por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha, etc;

III - data, hora e fuso horário, observando o previsto no art. 4° ; e

IV - endereço IP (Internet Protocol), porta de origem da conexão, identificador do ativo de informação, coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento.

Art. 6° Os ativos de informação que não permitem os registros dos eventos acima listados devem ser mapeados e documentados quanto ao tipo e formato de registros de auditoria permitidos e armazenados.

Art. 7° Os sistemas e redes de comunicação de dados devem ser monitorados, registrando-se, minimamente, os seguintes eventos de segurança, sem prejuízo de outros considerados relevantes:

I – utilização de usuários, perfis e grupos privilegiados;

II – inicialização, suspensão e reinicialização de serviços;

III – acoplamento e desacoplamento de dispositivos de hardware, com especial atenção para mídias removíveis;

IV – modificações da lista de membros de grupos privilegiados;

V – modificações de política de senhas, como por exemplo, tamanho, expiração, bloqueio automático após exceder determinado número de tentativas de autenticação, histórico, etc;

VI – acesso ou modificação de arquivos ou sistemas considerados críticos; e

VII – eventos obtidos por meio de quaisquer mecanismos de segurança existentes.

Art. 8° Recomenda-se que os ativos de informação sejam configurados de forma a armazenar seus registros de auditoria não apenas localmente, como também remotamente, por meio do uso de tecnologia aplicável.

CAPÍTULO V

DOS PROCEDIMENTOS PARA COLETA E PRESERVAÇÃO DE EVIDÊNCIAS

Art. 9° A Equipe responsável pelo tratamento de incidentes, deverá, sem prejuízo de outras ações, coletar e preservar:

I – as mídias de armazenamento dos dispositivos afetados ou as suas respectivas imagens forenses;

II – os dados voláteis armazenados nos dispositivos computacionais;

III – todos os registros de eventos citados no tópico 3.

Art. 10 Nos casos de inviabilidade de preservação das mídias de armazenamento mencionadas no inciso I, do art. 10, em razão da necessidade de pronto restabelecimento do serviço afetado, a equipe responsável deverá coletar e armazenar cópia dos arquivos afetados pelo incidente, tais como: logs, configurações do sistema operacional, arquivos do sistema de informação, e outros

julgados necessários, mantendo-se a estrutura de diretórios original e os "metadados" desses arquivos, como data, hora de criação e permissões.

Parágrafo único. A equipe responsável deverá fazer constar em relatório a eventual impossibilidade de preservação das mídias afetadas e listar todos os procedimentos adotados.

Art. 11 As ações de restabelecimento do serviço não devem comprometer a coleta e a preservação da integridade das evidências.

Art. 12 Para a preservação dos arquivos coletados, deve-se:

I - gerar arquivo contendo a lista dos resumos criptográficos de todos os arquivos coletados;

II - gravar os arquivos coletados, acompanhado do arquivo com a lista dos resumos criptográficos descritos no inciso anterior; e

III - gerar resumo criptográfico do arquivo a que se refere o inciso I.

CAPÍTULO VI

DA COMUNICAÇÃO DO INCIDENTE DE SEGURANÇA

Art. 13 Assim que tomar conhecimento do Incidente de Segurança em Redes Computacionais, deverá o responsável pelo setor afetado comunicar de imediato a equipe responsável com atribuição para apurar os fatos.

Art. 14 Após a conclusão do processo de coleta e preservação das evidências do incidente penalmente relevante, equipe responsável deverá elaborar Relatório de Comunicação de Incidente de Segurança em Redes Computacionais, descrevendo detalhadamente os eventos verificados.

§ 1° O Relatório de Comunicação de Incidente de Segurança em Redes Computacionais deverá ser instruído com as seguintes informações, sem prejuízo de outras julgadas relevantes:

I – o nome do responsável pela preservação dos dados do incidente, com informações de contato;

II - setor comunicante com sua localização e informações de contato;

III - número de controle da ocorrência;

IV - relato sobre o incidente, descrevendo como ocorreu, como foi detectado e quais dados foram coletados e preservados;

V - descrição das atividades de tratamento e resposta ao incidente e todas as providências tomadas pela equipe responsável, incluindo as ações de preservação e coleta, a metodologia e as ferramentas utilizadas e o local de armazenamento das informações preservadas;

VI - o resumo criptográfico citado no Art. 13°;

VII - Termo de Custódia dos Ativos de Informação Relacionados ao Incidente de Segurança;

VIII - justificativa sobre a eventual inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados, nos termos do parágrafo único, do Art. 11°.

Art. 15 Recebida a Comunicação de Incidente de Segurança em Redes Computacionais, a equipe responsável irá apurar os fatos, juntamente com o material coletado, para fins de instrução da notícia crime

CAPÍTULO VII

DISPOSIÇÕES FINAIS

Art. 16 Este protocolo deve ser revisado anualmente para garantir sua adequação às necessidades do **INSTITUTO DE TECNOLOGIA E INOVAÇÃO EVERESTE.**

Art. 17 Os casos omissos que seja preciso alterar, remover ou adicionar serão analisados pelo Comitê de Governança de Tecnologia da Informação e Comunicação.

EVERESTE

INSTITUTO DE TECNOLOGIA E INOVAÇÃO