ATO ADMINISTRATIVO Nº 032/2024/EVERESTE

Aprova o Protocolo de Prevenção a Incidentes 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 PREVENÇÃO A INCIDENTES 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 11:28:13 -04'00'

ANDRÉ FABIANO SANTOS PEREIRA

Presidente do Evereste

EVERESTE
INSTITUTO DE TECNOLOGIA E INOVAÇÃO

PROTOCOLO DE

PREVENÇÃO A INCIDENTES CIBERNÉTICOS

MANAUS
2024

SUMÁRIO

CAPÍTULO I

OBJETIVO

Art. 1° O Protocolo de Prevenção a Incidentes Cibernéticos tem como objetivo identificar, mitigar e proteger contra ameaças cibernéticas, responder rapidamente a incidentes e promover a conscientização e capacitação em segurança cibernética, com foco em:

I - Definir um conjunto de diretrizes para a prevenção de incidentes cibernéticos, visando minimizar os riscos e impactos decorrentes de possíveis ameaças à segurança da informação.

II - Garantir a conformidade com as regulamentações, normas e melhores práticas relacionadas à segurança cibernética, de forma a assegurar a integridade, confidencialidade e disponibilidade dos dados corporativos.

III - Promover medidas proativas que contribuam para a prevenção de incidentes cibernéticos e fortalecimento da resiliência do ambiente tecnológico, por meio de investimentos em tecnologias avançadas, treinamentos de conscientização e da equipe técnica.

CAPÍTULO II

CONSIDERAÇÕES IMPORTANTES

Art. 2° Este protocolo é parte do conjunto de Protocolos de Segurança Cibernética, ao qual também faz parte o Protocolo de Gerenciamento de Crises Cibernéticas e de Investigação de Ilícitos Cibernéticos.

Art. 3° As ações e medidas elencadas neste protocolo são complementares às políticas, aos processos, às práticas e aos procedimentos relacionados à segurança da informação já formalizados e estabelecidos no âmbito do **INSTITUTO DE TECNOLOGIA E INOVAÇÃO EVERESTE.**

CAPÍTULO III

FUNÇÕES DO PROTOCOLO DE PREVENÇÃO

Art. 4° As funções básicas que compõem este protocolo são: identificar, proteger, detectar, responder e recuperar:

I - A função **identificar** consiste em atividades para identificar ativos tecnológicos críticos, levantar, analisar e avaliar os riscos aos quais o ambiente tecnológico está exposto, possibilitando a priorização e concentração de recursos humanos, tecnológicos e financeiros de acordo com a criticidade. A função é contemplada pela seguinte atividade:

II - A função **proteger** consiste no desenvolvimento e implementação de controles que assegurem a proteção do ambiente tecnológico, dados (inclusive pessoais), além de contribuir para a eficiência e eficácia da prestação de serviços. No âmbito do **INSTITUTO DE TECNOLOGIA E INOVAÇÃO EVERESTE**, a função é contemplada pelas seguintes atividades:

a) Execução contínua do Sistema de Gestão de Segurança da Informação;

b) Gestão de Continuidade de TIC, formalizada na Política da Segurança da Informação; e

c) Realização de cópias de segurança do ambiente tecnológico, formalizada.

§1° Implementação de boas práticas de gerenciamento e proteção do ambiente tecnológico, observado normatizações e frameworks estabelecidos no mercado (como ABNT NBR 27002 e CIS Controls), tais como:

I - Gerenciamento de vulnerabilidades;

II - Implementação de soluções de segurança do ambiente (firewall, IPS, filtro de conteúdo web, proteção de endpoint, detecção e resposta de endpoint, dentre outras);

III - Hardening de serviços e de sistemas;

Art. 5° A função de **detectar** envolve a elaboração e aplicação de medidas destinadas à identificação de eventos e/ou incidentes de segurança cibernética. **Art.**

Art. 6° A função **responder** compreende a definição e implementação de medidas visando uma resposta ágil e eficaz a tais incidentes.

Art. 7° A função **recuperar** diz respeito ao desenvolvimento, implementação e manutenção de planos e ações para prover resiliência e capacidade de recuperação aos serviços, sistemas e ativos tecnológicos em caso de ocorrência de eventos e/ou incidentes de segurança cibernética.

Art. 8° Essas três funções estão contempladas pelas seguintes atividades:

I - Gestão de Incidentes de Segurança da Informação;

II - Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação;

III - Gestão de Continuidade de TIC.

CAPÍTULO IV

BENEFÍCIOS DE SUA IMPLEMENTAÇÃO

Art. 9° Este protocolo de prevenção a incidente cibernéticos busca trazer os seguintes benefícios:

I - Fortalecer as iniciativas de tratativa de incidentes cibernéticos;

II - Elevar o nível de segurança cibernética do ambiente tecnológico; e

III - Adotar boas práticas e requisitos de segurança cibernética.

CAPÍTULO V

CONSIDERAÇÕES FINAIS

Art. 10 Caso surjam evidências de atividades criminosas durante a resolução de incidentes de segurança cibernética, é necessário seguir, além das ações mencionadas ou referenciadas neste protocolo, as diretrizes estabelecidas no Protocolo de Investigação de Ilícitos Cibernéticos. Esse procedimento é fundamental para assegurar a conformidade legal e o tratamento adequado de tais situações, garantindo a integridade das informações e dos sistemas envolvidos.

Art. 11 Este protocolo entra em vigor na data de sua publicação e deve ser revisado anualmente para garantir sua adequação às necessidades do **INSTITUTO DE TECNOLOGIA E INOVAÇÃO EVERESTE.**

Art. 12 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

WWW.EVERESTE.ORG.BR