ATO ADMINISTRATIVO Nº 033/2024/EVERESTE

Aprova o Protocolo de Gerenciamento de Crise Cibernética 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 GERENCIAMENTO DE CRISE CIBERNÉTICA** 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 12:16:11 -04'00'

ANDRÉ FABIANO SANTOS PEREIRA

Presidente do Evereste

EVERESTE
INSTITUTO DE TECNOLOGIA E INOVAÇÃO

PROTOCOLO DE

GERENCIAMENTO DE CRISE CIBERNÉTICA

MANAUS
2024

SUMÁRIO

CAPÍTULO I

OBJETIVO

Art. 1° Estabelecer um conjunto de diretrizes para responder efetivamente a crises decorrentes de incidentes cibernéticos. Promover adequação e alinhamento às regulamentações, normas e melhores práticas relacionadas à segurança cibernética.

CAPÍTULO II

CONSIDERAÇÕES IMPORTANTES

Art. 2° As ações e medidas mencionadas neste protocolo são complementares às políticas, processos, práticas e procedimentos já formalizados e estabelecidos no âmbito do Instituto Evereste, relacionados à segurança da informação.

Art. 3° Este protocolo deve ser acionado nos casos em que as medidas estabelecidas no Protocolo de Prevenção de Incidentes Cibernéticos não forem suficientes para evitar a ocorrência de um incidente.

Art. 4° Para efeitos deste protocolo, são considerados críticos para o funcionamento do Instituto Evereste os seguintes sem:

I - Software de Service Desk

II - Software de Reconhecimento Facial

III - Software de Gerenciamento de Atividades e Projetos

Art. 5° Uma crise cibernética surge quando um evento ou uma série de eventos danificam os sistemas críticos de uma organização. Esses eventos têm propriedades emergentes que excedem as habilidades de uma organização para lidar com as demandas que eles geram. Além disso, esses eventos têm implicações significativas para a organização e seus constituintes, direta ou indiretamente.

Art. 6° Os atores atuantes ativamente no gerenciamento de crises cibernéticas do Instituto Evereste, cujas atribuições serão definidas pelo Comitê de Governança de Tecnologia da Informação e Comunicação.

CAPÍTULO III

IDENTIFICAÇÃO DE UMA CRISE CIBERNÉTICA

Art. 7° A identificação de uma crise cibernética ocorre por meio de indicadores como atividades suspeitas na rede, alertas de segurança, comportamento anormal de sistemas e relatórios de usuários. É crucial ter uma equipe de resposta a incidentes treinada para identificar e investigar esses indicadores, visando uma pronta ação diante da crise.

§ 1º Algumas das atividades são:

I. Interrupções ou indisponibilidade dos sistemas de TI essenciais.
II. Comportamento anormal dos dispositivos, como reinicializações frequentes, lentidão extrema ou atividade excessiva da rede sem explicação.
III. Tentativas de acesso não autorizado a sistemas ou dados confidenciais.
IV. Roubo ou comprometimento de dados, incluindo informações pessoais, financeiras ou segredos comerciais.
V. Detecção de malware nos sistemas de TI, como vírus, cavalos de Tróia ou ransomware.
VI. Ataques DDoS, com grande volume de tráfego malicioso direcionado aos sistemas, resultando em indisponibilidade de serviços online.
VII. Recebimento de comunicações suspeitas relacionadas à segurança cibernética, como ameaças, chantagens ou solicitações de informações confidenciais.

CAPÍTULO IV

GERENCIAMENTO DE CRISES CIBERNÉTICAS

Art. 8° O gerenciamento de crise cibernética se inicia quando:

I - ficar caracterizado grave dano material ou de imagem;

II - restar evidente que as ações de resposta ao incidente cibernético provavelmente perdurarão por longo período, podendo se estender por dias, semanas ou meses;

III - o incidente impactar gravemente os serviços de TIC essenciais ao funcionamento do **INSTITUTO DE TECNOLOGIA E INOVAÇÃO EVERESTE**, extrapolando os limites determinados nas diretrizes do plano de continuidade de TIC;

IV - atrair grande atenção da mídia e da população em geral; ou

V - ocorrer incidentes de segurança com dados pessoais.

Art. 9º Confirmada a crise cibernética, tem-se:

I - Caso seja identificada uma crise envolvendo dados pessoais, o Encarregado de Tratamento de Dados Pessoais do Instituto Evereste deverá notificar as entidades externas, cumprindo os requisitos previstos na Lei Geral de Proteção de Dados (LGPD) e quaisquer outras normas de proteção de dados pessoais aplicáveis no Instituto Evereste.

II - Para o tratamento do incidente que ocasionou a crise, deverão ser utilizadas políticas, planos de resposta a incidentes, planos de continuidade e de recuperação de desastres e procedimentos técnicos já elaborados e formalizados.

III - A crise encerra-se no momento em que for constatado o retorno à normalidade das operações.

IV - Deve ser elaborado um relatório da crise com o intuito de registrar as ações que foram efetivas e as melhorias necessárias para corrigir as causas do incidente que originou a crise (lições aprendidas). O relatório deve conter as seguintes informações:

a) identificação e análise da causa-raiz do incidente;
b) a linha do tempo das ações realizadas;
c) a escala do impacto nos dados, sistemas e operações de negócios importantes durante a crise;
d) os mecanismos e processos de detecção e proteção existentes e as necessidades de melhoria identificadas; e
e) As ações realizadas para tratamento da crise e avaliação de sua eficácia.

CAPÍTULO V

DURANTE UMA CRISE

Art. 10. A comunicação entre todas as áreas envolvidas em uma crise é fator crítico para uma organização responder a uma crise cibernética de longa duração ou de grande impacto.

Art. 11 Para melhorar a eficácia do trabalho do Comitê de Governança de Tecnologia da Informação e Comunicação, é necessário:

I - entender claramente o incidente que gerou a crise, sua gravidade e os impactos negativos;

II - levantar todas as informações relevantes, verificando fatos e descartando boatos;

III - levantar soluções alternativas para a crise, apreciando sua viabilidade e suas consequências;

IV - avaliar a necessidade de suspender serviços e/ou sistemas informatizados;

V - centralizar a comunicação na figura de um porta-voz para evitar informações equivocadas ou imprecisas;

VI - realizar uma comunicação tempestiva e eficiente, de forma a evidenciar o trabalho diligente das equipes e a enfraquecer boatos ou investigações paralelas que alimentem notícias falsas;

VII - definir estratégias de comunicação com a imprensa e/ ou redes sociais e estabelecer qual a mídia mais adequada para se utilizar em cada caso;

VIII - aplicar o Protocolo de Investigação para Ilícitos Cibernéticos do INSTITUTO EVERESTE;

IX - solicitar a colaboração de especialistas ou de centros de resposta a incidentes de segurança;

X - fornecer aconselhamento sobre as prioridades e estratégias da organização para uma recuperação rápida e eficaz;

XI - definir os procedimentos de compartilhamento de informações relevantes para a proteção de outras organizações com base nas informações colhidas sobre o incidente; e

XII - elaborar plano de retorno à normalidade.

Art. 12 As etapas e procedimentos de resposta são diferentes a depender do tipo de crise e são necessárias reuniões regulares para avaliar o progresso até que seja possível retornar à condição de normalidade.

CAPÍTULO VI

FASE DE APRENDIZAGEM E REVISÃO (PÓS CRISE)

Art. 13 Quando as operações retornarem à normalidade, o Comitê de Governança de Tecnologia da Informação e Comunicação deverá realizar a análise criteriosa das ações tomadas, observando as que foram bem-sucedidas e as que ocorreram de forma inadequada.

Art. 14 Para a identificação das lições aprendidas e a elaboração do relatório final, deve ser objeto de avaliação todos os tópicos abordados no Art. 10° - inciso IV.

CAPÍTULO VII

CONSIDERAÇÕES FINAIS

Art. 15 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

WWW.EVERESTE.ORG.BR