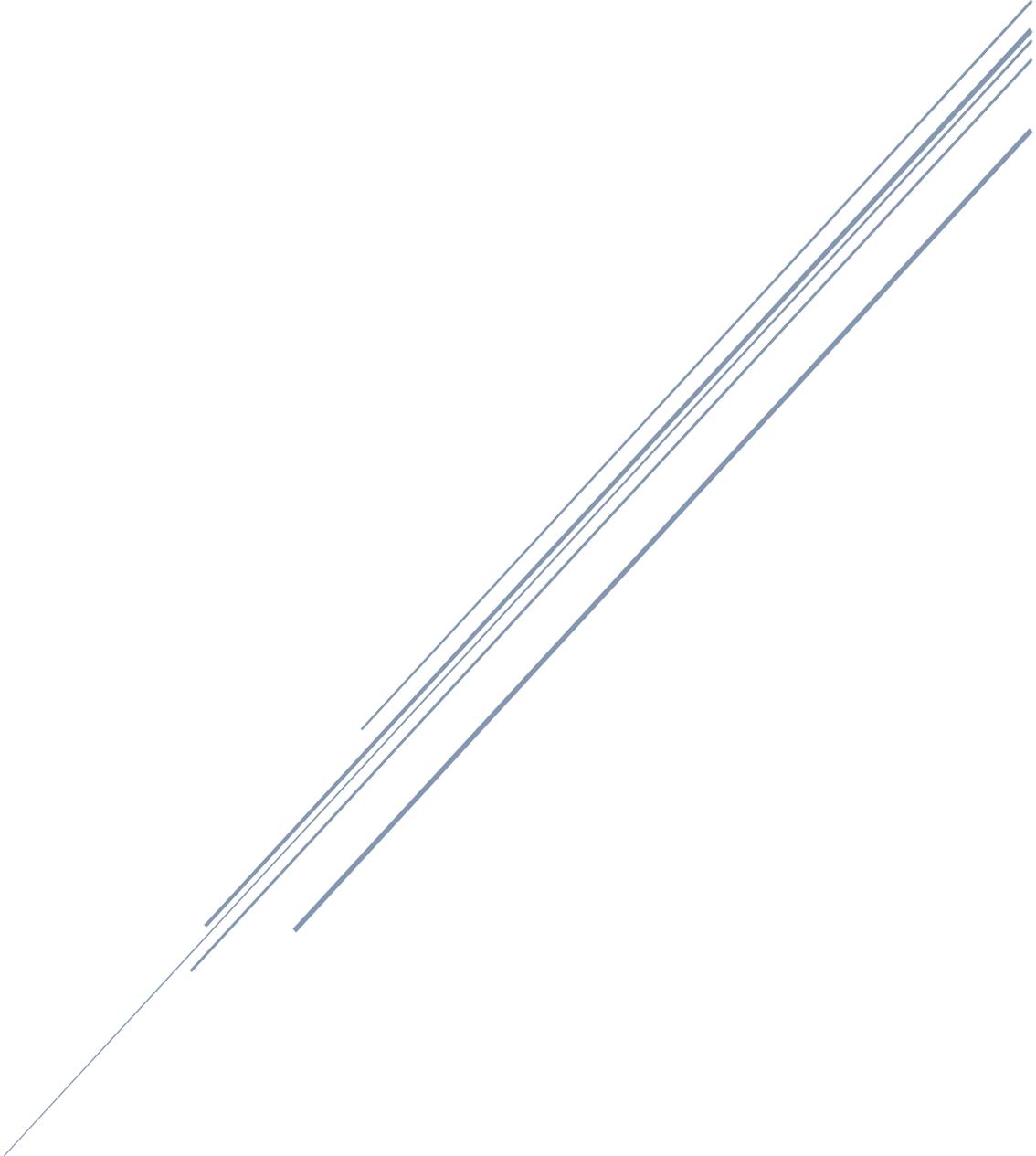


PROGRAMA DE CONSCIENTIZAÇÃO E CAPACITAÇÃO EM SEGURANÇA DA INFORMAÇÃO DO TRE-ES



1.0
2023

HISTÓRICO DE REVISÕES

VERSÃO	DATA	DESCRIÇÃO	AUTOR
1.0	04/05/2023	Criação do documento	Olga Bayerl vita
1.0	12/05/2023	Revisão, Ajuste e Atualização	Sandro Merçon

Sumário

1 Introdução.....	3
2 Objetivo	4
3 Escopo	5
4 Conceitos e definições.....	6
5 Estrutura do programa	6
6. Conteúdos.....	6
7 Periodicidade.....	7
8 Competências e responsabilidades.....	8

1 Introdução

O Tribunal Regional Eleitoral do Espírito Santo (TRE-ES) vem consolidando uma infraestrutura tecnológica cada vez mais robusta e eficiente, em resposta a demandas por modernização, informatização e transformação digital que visam aprimorar os serviços jurisdicionais prestados ao cidadão.

O crescimento da infraestrutura tecnológica traz consigo um grande desafio que é a manutenção de um ambiente computacional seguro, que garanta a confidencialidade, a integridade e a disponibilidade das informações, em especial dos dados pessoais.

Nessa linha, há duas frentes extremamente importantes a serem seguidas. A primeira diz respeito à aquisição de soluções tecnológicas modernas capazes de identificar vulnerabilidades, ataques e criar camadas adicionais de segurança. E a segunda, objeto deste programa, trata diretamente da capacitação da Alta Gestão, das equipes de tecnologia, dos usuários e de toda a comunidade institucional quanto à importância da cibersegurança e às boas práticas de proteção de dados. A conscientização e o treinamento constantes são fundamentais para mitigar riscos e fortalecer a cultura de segurança da informação dentro do TRE-ES.

A capacitação da Alta Gestão envolve o entendimento das ameaças cibernéticas em constante evolução e a incorporação das medidas de segurança no planejamento estratégico da instituição. É essencial que os gestores estejam cientes dos desafios e das melhores práticas em cibersegurança, aprimorando a tomada de decisão e garantindo recursos humanos e financeiros adequados para a Segurança da Informação.

Além disso, é imprescindível que as equipes de tecnologia sejam capacitadas para implementar e gerenciar soluções de segurança eficazes. Isso inclui a atualização constante de conhecimentos sobre novas ameaças, técnicas de detecção e prevenção, além de promover testes regulares de vulnerabilidade e auditorias de segurança nos sistemas do TRE-ES.

A conscientização dos usuários finais também desempenha um papel crucial na proteção da infraestrutura tecnológica. Através de programas de treinamento e campanhas de conscientização, os funcionários, estagiários e colaboradores são educados sobre as práticas seguras de uso dos sistemas, como o uso de senhas robustas, a identificação de e-mails e links suspeitos, e a importância de manter os dispositivos atualizados.

A capacitação contínua de toda a comunidade institucional do TRE-ES, desde a Alta Gestão até os usuários finais, é um investimento estratégico para fortalecer a segurança cibernética e garantir a proteção dos dados pessoais e a confiabilidade dos serviços oferecidos ao cidadão.

2 Objetivo

O Conselho Nacional de Justiça definiu, como parte da Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-JUD), a Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário - PECSC-PJ, que tem como objetivos:

a) propiciar o constante aprimoramento dos níveis de segurança cibernética nos ativos e serviços de Tecnologia da Informação e Comunicação nos órgãos do Poder Judiciário;

b) inserir o tema da segurança cibernética como tópico estratégico e primordial a constar das pautas institucionais de todos os órgãos do Poder Judiciário;

c) promover a elevação do grau de conhecimento e de consciência quanto à cultura da segurança da cibernética no âmbito do Poder Judiciário;

d) assegurar que todo usuário dos serviços de informação do Poder Judiciário tenha a devida compreensão de suas responsabilidades na proteção das informações dos órgãos do Poder Judiciário; Secretaria de Tecnologia da Informação Estratégia Nacional de Capacitação em Cibersegurança TSE e TREs – 2021 a 2024 Versão 2.0 Página 6 de 14;

e) assegurar que novos conhecimentos atinentes ao tema da segurança cibernética sejam permanentemente ofertados aos profissionais das áreas de Tecnologia da Informação e Comunicação e de Segurança da Informação, em nível acadêmico, técnico, gerencial, entre outros aplicáveis.

Este documento institui o Programa de Conscientização em Segurança Cibernética do Tribunal Regional Eleitoral do Espírito Santo (TRE-ES), alinhado ao PECSC-PJ.

O Programa que tem como principal objetivo promover a conscientização e o treinamento de todos os envolvidos na instituição, desde a Alta Gestão até os usuários finais, sobre a importância da cibersegurança e a adoção de boas práticas de proteção de dados, através de ações e iniciativas concretas. Traz como proposta conteúdos variados sobre o tema da Segurança da Informação em diversos níveis e abordagens. Busca mobilizar quanto à importância de um comportamento digital seguro e trabalhar a consciência das pessoas em relação ao valor da informação, garantindo assim a confiabilidade nos processos de trabalho da instituição.

Conscientizar é conquistar para que todos possam colaborar de forma espontânea e comprometida com a segurança da informação no TRE-ES.

3 Escopo

Este programa aplica-se no âmbito do TRE-ES a toda comunidade institucional. As ações do PCCSI-TRE/ES serão realizadas de forma continuada, buscando sempre a capacitação em Segurança da Informação aplicada na utilização dos recursos e serviços de Tecnologia da Informação.

4 Conceitos e definições

- a) Conformidade em SI: cumprimento das legislações, normas e procedimentos relacionados à Segurança da Informação e Comunicações da organização;
- b) Conscientização em SI: ações educativas que impactam na mudança de postura e de comportamento com relação a SI.
- c) Atividades de capacitação em SI: qualquer atividade que envolva ação direta de orientação, treinamento, capacitação, conscientização descritas neste programa.
- d) Boas práticas em SI: práticas e competências básicas em Segurança da Informação reconhecidas amplamente pelo mercado, compreendendo comportamentos e procedimentos desempenhados no ambiente profissional. Aplica-se em campos específicos e podem ser disseminados.
- e) Cursos introdutórios em SI: cursos de básicos sobre um tema referente a um assunto da área de SI.
- f) Cert.br - O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil é mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil, e atende a qualquer rede brasileira conectada à Internet

5 Estrutura do programa

O PCCSI-TRE/ES se desenha como uma iniciativa de conscientização e capacitação em SI através de palestras, minicursos, cursos/capacitações, tanto no formato presencial como em plataformas de EAD.

Além disso, engloba o programa a produção, publicação e veiculação de material informativo em diversas mídias de comunicação com o intuito de ampliar o alcance das iniciativas.

6. Conteúdos

O conteúdo do programa continuado contempla:

- a) Informativos - a divulgação dos Boletins Informativos Mensais de Segurança da Informação elaboradas pelo Cert.br, no site do Núcleo de Segurança Cibernética (NSC);
- b) Conscientização – Cursos, cartilhas, palestras, boletins e campanhas contendo treinamentos voltados para a conscientização e orientação sobre segurança da informação, fazendo com que os participantes saibam aplicar os conhecimentos em sua rotina pessoal e profissional, além de servirem como multiplicadores sobre o tema. As ações de conscientização deverão ser prestadas de forma contínua e os resultados deverão ser analisados criticamente para que este programa possa estar sempre alinhado com os objetivos deste Tribunal;
- c) Campanhas de phishing – Testes de phishing realizados utilizando plataforma específica, KnowBe4, a fim de detectar usuários que precisam de mais ações de treinamento e conscientização;
- d) Capacitação – Cursos e palestras especializados voltados para públicos específicos, conforme estabelecido na Estratégia Nacional de Capacitação em Cibersegurança, além da criação de trilhas de cursos para a equipe técnica em plataformas de treinamento do mercado.
- e) Atividades de Comunicação - As atividades de comunicação abrangerão ações voltadas para o acesso à informação de maneira imediata pelos usuários através de um ou mais canais de comunicação oficiais do TRE-ES, a saber: correio eletrônico, intranet, “Participando”, site do núcleo de segurança, plataforma de conscientização KnowBe4, etc.

7 Periodicidade

Informativos: lançamento de pelo menos 1 informativo mensal no site do NSC.

Conscientização: ao menos 3 eventos anuais de conscientização podendo ter o formato de palestra ou curso de conscientização; lançamento mensal de cartilhas ou boletins de segurança no site do NSC.

Campanhas de phishing: realização de ao menos uma campanha por mês, podendo envolver todos os usuários ou grupos específicos.

Capacitação: programação de ao menos um curso especializado de capacitação, por ano, para as equipes especializadas em segurança da informação: NSC e ETIR. Cursos específicos para capacitação da STI disponibilizados na plataforma Udemy, ou contratados de outra entidade.

Atividades de comunicação: lançamento mensal de pílulas de segurança no “Participando”; e-mails de orientação produzidos pela CIS; resposta aos e-mails reportados como phishing, de forma a orientar os usuários se realmente trata-se de phishing; atualização mensal da página do NSC com mais informações de SI.

8 Competências e responsabilidades

Cabe à Alta Administração reconhecer a importância da segurança cibernética como um aspecto crítico da governança corporativa e do gerenciamento de riscos. Apoiar e incentivar as ações do programa, fornecendo liderança, recursos, direção estratégica e exemplo para toda a organização. Seu envolvimento ativo e comprometimento são essenciais para criar uma cultura de segurança cibernética sólida e eficaz.

Cabe ao Gestor de Segurança da Informação do Tribunal desenvolver e planejar estrategicamente o programa de conscientização em segurança cibernética, envolvendo a definição de metas, objetivos e abordagens educacionais para promover uma cultura de segurança cibernética dentro da organização.

Cabe ao Núcleo de Segurança Cibernética da Coordenadoria de Infraestrutura Tecnológica e Segurança Cibernética a condução efetiva das ações, coordenando a produção, o desenvolvimento e aplicação das iniciativas, interagindo com a Escola Judiciária Eleitoral no que couber.