ASSEMBLEIA LEGISLATIVA DE PERNAMBUCO (ALEPE)
Escola do Legislativo de Pernambuco (Elepe)
Ouvidoria (Ouvleg)
Superintendência de Tecnologia da Informação (STI)

CONTEÚDO DO CURSO

MÓDULO 1 – FUNDAMENTOS DE SEGURANÇA DA INFORMAÇÃO | 6 HORAS

1.1 Conceitos

- Estamos seguros?
- Segurança da Informação (SI)
- A cebola
- Normas associadas à SI
- A tríade da SI
- AAA
- Privilégio Mínimo
- Autenticação de Múltiplos Fatores
- Criptografia
- Controles de Acesso

1.2 Principais Tipos de Ataques

- Engenharia Social
- Ataques a senhas (força bruta, dicionário)
- Negação de Serviço
- Malwares (ransomware, trojan, spyware, vírus, keylogger)

1.3 Política de Segurança da Informação da ALEPE

- Objetivos
- Princípios e Diretrizes
- Estrutura da Gestão da SI
- Diretrizes para as normas, políticas e procedimentos

MÓDULO 2 – FUNDAMENTOS DA PROTEÇÃO DE DADOS PESSOAIS | 6 HORAS

2.1 Conceitos introdutórios

- Dado, informação e conhecimento
- Dados Pessoais
- Dados Pessoais Sensíveis
- Agentes de Tratamento

2.2 Sistema Brasileiro de Proteção de Dados Pessoais

- Por que proteger dados pessoais?
- Privacidade, Intimidade e Dados Pessoais
- Breve histórico das principais normas relacionadas à proteção de dados pessoais (LAI, MCI, LGPD e EC 115/2022)
- Harmonização entre LGPD e LAI
- Enunciados da CGU

2.3 Tratamento de dados pessoais de acordo com a LGPD

- Princípios
- Hipóteses para o tratamento de dados pessoais
- Tratamento de Dados Pessoais Sensíveis
- Tratamento de Dados no Setor Público
- Direitos do Titular
- Boas práticas
- Incidentes de segurança
- Fiscalização e Sanções
- Peculiaridades do tratamento de dados no Poder Legislativo
- Política de Proteção de Dados Pessoais da Alepe

MÓDULO 3 – APLICAÇÕES PRÁTICAS DE SEGURANÇA DIGITAL | 12 HORAS

3.1 Proteção de Contas e Autenticação Segura

- Configuração de autenticação em dois fatores (2FA)
- WhatsApp: Proteção contra sequestro de contas e clonagem de WhatsApp
- E-mail
- Redes sociais: Instagram, Facebook e demais aplicações web
- SMS
- Uso de aplicativos de autenticação segura (Authenticator, Microsoft Authenticator, Google Authenticator)
- Gerenciamento seguro de senhas: boas práticas, uso de gerenciadores confiáveis e política de senhas fortes
- Reconhecimento e mitigação de tentativas de golpes e engenharia social

3.2 Segurança de Dispositivos Móveis e Aplicações

- Configurações essenciais para proteção de celulares e tablets (Android e iOS)
- Uso seguro de aplicativos bancários e de comunicação
- Ferramentas e serviços para proteção pessoal e institucional:
    - Rede Sim (proteção do CPF)
    - Registrato (monitoramento de contas bancárias e crédito)
    - Celular Seguro e Alerta Celular (rastreamento e bloqueio de dispositivos)
    - Não Me Perturbe (bloqueio de ligações indesejadas)
- Verificação de vazamento de dados pessoais e jurídicos

    - Ferramentas de monitoramento (Google Alerts, Firefox Monitor, Have I Been Pwned)
- Pesquisa em fontes abertas (OSINT) para análise da exposição de informações
    - Métodos básicos para busca de informações públicas
    - Identificação de dados sensíveis disponíveis em redes sociais e sites de terceiros

3.3 Navegação, identificação e compras online

- Verificação de perfis, websites, lojas online
- Pesquisa em fontes abertas (OSINT) para análise da exposição de informações
    - Métodos básicos para busca de informações públicas
    - Identificação de dados sensíveis disponíveis em redes sociais e sites de terceiros
- Aparelho celular: Biometria, senha ou digital
- Proteção de crianças e adolescentes: Controle parental
- Testes práticos de autenticação segura
- Recuperação de contas comprometidas: WhatsApp e Redes Sociais
- Uso seguro de aplicativos bancários e de comunicação. PIX.