**ADMINISTRAÇÃO, TI, CONTÁBIL**

**Boas Práticas de segurança da informação em ambientes computacionais do Sistema CFN/CRN**

**Palestrante: Vinícius Bonfim (CFN)**

**Data: 20/07/2017**

**Hora: 11h50 – 13h**

O palestrante Bonfim é assessor de TI no CFN. Ele começa a palestra, mencionando os benefícios do SEI, apresentado na palestra anterior. A palestra começa com um alerta sobre o perigo da dependência absoluta no computador.

A palestra se introduz com Bonfim expondo uma matéria do portal G1 sobre um ataque de hackers. A ameaça de hackers afeta os Conselhos Regionais, é preciso investir em tecnologia e segurança.

Assim, o palestrante expõe gráficos que mostram o aumento na quantidade de computadores e aparelhos móveis ativos no Brasil. Da década de 80 até hoje, nós mudamos nossa forma de trabalhar, comunicar e armazenar informações, o palestrante afirma que as mudanças estão ocorrendo muito rápido e por isso estamos despreparados para lidar com os problemas que podem surgir.

O CFN possui 495 GB de informações e dados de 121893 nutricionistas. O palestrante cita as ofertas de compra de dados ao Conselhos, prática criminosa.

Conforme o número de pessoas utilizando computadores conectados à internet aumenta, os riscos se ampliam. É mostrado gráfico que mostra o aumento de riscos na internet. Em 2016, a *Karpersky Lab* detectou 8526221 pacotes de instalações maliciosas. São mostradas várias chamadas de notícias sobre ataques de hackers.

Palestrante cita vários casos de invasão. Um conselho regional de corretores de imóveis, cujos dados estavam na página PasteBIN, foi invadido. O site do CFN foi invadido mais de uma vez. O site de *incorpatch* foi invadido também. O governo de São Paulo foi hackeado contra a violência policial.

Porém, o palestrante afirmou que existe um caminho. Os pilares da segurança da informação são: confidencialidade; integridade; disponibilidade; autenticidade; não-repúdio.

O palestrante cita um caso de ataque aos dados no CFN, e frisa que os integrantes do Conselho não são orientados a lidar e se proteger, sendo que orientar as pessoas é algo essencial para proteger os dados. A solução não pode focar apenas em tecnologia, mas também na orientação das pessoas.

Houve a normatização das políticas de segurança do CFN, que afirma que: recurso tecnológicos e informação pertencem ao Conselho; orientação quanto a natureza confidencial das informações obtidas pelo colaborador; os recurso de TI são pautados pela responsabilidade, ética, economia, licitude e boa-fé; recursos tecnológicos sensíveis são pessoais e intransferíveis; esclarecimentos quando auditorias.

É imprescindível investir em tecnologia, inclusive Firewall e antivírus empresariais. O Firewall do CFN ou CRN custou R$7500,00 e a manutenção custa R$ 390,00. O antivírus do CFN ou CRN custa R$ 23,50 por máquina.

Deve-se fazer auditoria, verificando os procedimentos e controles de segurança dos dados, e ter políticas de backup e armazenamento e atualizações obrigatórias, que repara problemas e vulnerabilidades. Também deve-se investir softwares originais, para que haja riscos do computador ser contaminado.

Phishing é uma forma que criminosos utilizam para você dar informações pessoais, palestrante cita casos pessoais e alerta da importância de checar o endereço das páginas que você acessa.

É importante que as pessoas tenham sejam fortes, que sejam fáceis de lembrar e não usem palavras reais.

A palestra é concluída com a seguinte informação: uma estimativa da Cyberventures afirma que os danos causados por crimes virtuais já causaram bilhões em gastos em dinheiro.