Participantes:
Hebert, Antonio Ferreira, Gualter Gonçalves, Rosileia Moraes, Daniele Cavaignaic, Wellington Silva, Alysson Cristiano,

Reunião CSI em 14/02/2021

- **Ações de comunicação que deverão ser feitas:**
  - Realizar via e-mail, mídias sociais, whatsapp
  - Dar destaque ao portal da segurança
  - Banner na página principal
  - Janela tipo pop up
- **Assuntos**:
  - Uso de senhas
  - Utilização de pen-drive
  - Bloqueio de tela ao deixar computador sozinho
  - Navegação segura na internet
  - Uso de redes sociais
    - Não confie em estranhos na internet
  - SPAM
  - Dicas de segurança na internet
  - Ransomware
  - PHISING
  - Códigos maliciosos
  - Boatos
  - Comércio eletrônico
  - Computadores
  - Dispositivos móveis:
    - Cuidado com aplicativos falsos
    - Cuidado com os dispositivos
    - Mantenha atualizado
    - Não clique em tudo que receber
  - Internet Bank
  - Comércio Eletrônico
    - Arrependimento em compras on-line
    - Verifique o vendedor
    - Navegação segura
  - Privacidade
  - Proteção de Dados
    - Backup
    - Senhas seguras
    - Senhas variáveis
    - Gerenciador de senhas
    - Verificação em dois fatores
    - Compartilhamento de informações
  - Vazamento de dados
    -

- - Ações de aquisição:
  - Antivírus
  - Cofre de senhas
  - Hiperconvergência
  -

- Ações de construção de diretrizes:
  - Plano de Continuidade de TIC
    - Inventário de ativos

- Plano de Resposta a Incidentes Cibernéticos
- Definição de Ativos Críticos
- Levantamento de Riscos de Ativos Críticos
- Plano de Comunicação:
  - Feita através de canal oficial do TRE-MA
  - Montar resposta juntamente com Comitê de Crise Cibernética
  - Definir quais informações poderão ser compartilhadas com parceiros
  - Designar pessoas para fazer contato com pessoas externas para aliviar a pressão sobre as equipes técnicas
  - Contratar consultoria/treinamento
  -
- Plano de Contratação: definir regras para aquisições emergenciais
-
-

- Adequação da Norma da ETIR aos normativos do CNJ e TSE
- Analisar propostas para alteração de acesso VPN
  - Acesso à VPN por padrão será bloqueado de segunda a sexta-feira durante a noite (a partir das 22h até às 6h da manhã). As exceções serão tratadas pelo DG;
  - A solicitação deverá ser feita pelo Gestor Máximo da Unidade através de SEI direcionado para a SERED;
  - A revalidação do acesso ocorrerá em meses fixos (janeiro, abril, julho e outubro) para facilitar a operacionalização por parte da Sered devido a limitações da ferramenta de VPN. Nestes meses os acessos serão bloqueados sendo necessário envio de SEI solicitando a renovação do acesso;
  - O fiscal de contrato pode solicitar acesso temporário VPN para prestadores de suporte enviando SEI direcionado à COINF devendo o serviço ser acompanhado pelo fiscal. Esse acesso não poderá ultrapassar 12h de acesso contínuo;
  - Para que ocorra a autenticação da conta de usuário atualmente é enviado um token (código) para o email institucional. Ocorre que a senha de email da conta de usuário é a mesma do e-mail institucional e, portanto, se a conta de usuário for comprometida o atacante terá acesso ao e-mail institucional e poderá recuperar o token para acessar a VPN. A modificação proposta é que seja enviado o token para um email externo à Justiça Eleitoral que possui senha diferente da senha institucional.
-

-