Política de Segurança da Informação

Última Atualização 01 de Dezembro de 2025

A Política de Segurança da Informação da WiFi no Evento, marca operada pela CDAtech, estabelece princípios, diretrizes, controles e procedimentos adotados para garantir confidencialidade, integridade, disponibilidade, privacidade, proteção de dados e segurança operacional em todas as soluções de conectividade, monitoramento e controle de acesso fornecidas para eventos, feiras, congressos e ambientes corporativos.

A WiFi no Evento aplica padrões profissionais de engenharia de redes, segurança cibernética e proteção de dados, sob a responsabilidade técnica direta do especialista Moacir Havlock, responsável exclusivo pela gestão e supervisão de todas as operações de segurança.

1. OBJETIVO DA POLÍTICA

Garantir que todos os usuários, dispositivos, sistemas e serviços operados ou disponibilizados pela CDAtech sejam protegidos contra:

- acessos indevidos
- tentativas de interceptação
- ataques cibernéticos
- roubo de dados
- invasão lateral entre usuários
- falhas de rede
- vulnerabilidades do ambiente de evento

O objetivo central é assegurar que cada pessoa conectada à rede WiFi no Evento esteja totalmente protegida, mesmo em um ambiente de alta densidade e risco elevado, típico de redes públicas.

2. PRINCÍPIOS FUNDAMENTAIS

A WiFi no Evento implementa sua Política de Segurança baseada nos seguintes princípios:

- Isolamento completo entre usuários
- Zero confiança (Zero Trust)
- Mínimo privilégio

- Compartimentação de redes (VLANs, ACLs, segmentação lógica e física)
- Criptografia sempre que aplicável
- Rastreabilidade e auditoria
- Prevenção de ameaças e detecção proativa
- Conformidade com a LGPD e o Marco Civil da Internet

3. ISOLAMENTO AVANÇADO DOS USUÁRIOS – PRINCIPAL MEDIDA DE SEGURANÇA

Este é o pilar da WiFi no Evento e deve ficar claro para usuários e organizadores:

3.1. Isolamento total entre dispositivos

A rede WiFi da CDAtech utiliza tecnologias de isolamento que impedem completamente que um usuário veja, visualize, detecte ou comunique-se com outro usuário conectado à mesma rede, incluindo:

- Client Isolation (AP-level isolation)
- Port Isolation
- AP Isolation + L2 Filtering
- Filtragem ARP e DHCP (anti-spoofing)
- Proteção contra scans (Nmap, Fing, ARP Scan)
- Bloqueio de tráfego lateral (east-west traffic)
- Inspeção e bloqueio de multicast e broadcast indevidos

3.2. Justificativa técnica

Ambientes de eventos são altamente vulneráveis porque em redes públicas convencionais:

- um usuário pode visualizar dispositivos próximos
- é possível tentar capturar dados de outros
- apps de "scanner" identificam celulares, notebooks e IPs
- atacantes podem tentar interceptar tráfego local
- é possível explorar brechas de redes abertas

Na WiFi no Evento isso não acontece, pois:

- ✓ Cada usuário está logicamente isolado
- ✓ Não existe comunicação entre clientes
- ✓ O dispositivo de um usuário é invisível para todos os outros
- ✓ Não há riscos de exploração lateral

3.3. Resultado prático

- Um dispositivo malicioso não pode ver outros dispositivos
- Não é possível realizar ataques de spoofing
- Não há como capturar tráfego alheio
- A experiência é tão segura quanto rede corporativa de alta segurança

4. ARQUITETURA DE REDE SEGURA

A WiFi no Evento utiliza uma arquitetura profissional composta por:

4.1. Redes segmentadas

- Rede visitante
- Rede expositores
- Rede staff
- Rede pagamentos

Cada rede opera em VLANs separadas, sem tráfego cruzado.

4.2. Firewalls dedicados

Com:

- inspeção profunda de pacotes
- bloqueio de portas indevidas

- IPS/IDS
- políticas de acesso mínimo

4.3. Access Points de padrão empresarial
Com:
- WPA3/Enterprise quando aplicável
- proteção anti-rogue AP
- airtime fairness
- controle de interferência
- load balancing inteligente

5. MONITORAMENTO E DETECÇÃO DE AMEAÇAS
Toda a rede é monitorada em tempo real pelo especialista Moacir Havlock, com:
- análise de espectro
- detecção de APs falsos (rogue APs)
- detecção de ataques de desautenticação
- detecção de spoofing e man-in-the-middle
- monitoramento de carga, latência e performance

6. PROTEÇÃO DE DADOS E PRIVACIDADE
A WiFi no Evento cumpre rigorosamente:
- LGPD (Lei 13.709/2018)
- Marco Civil da Internet (Lei 12.965/2014)
- Decreto 8.771/2016

Os dados coletados são apenas os necessários para:
- autenticação
- segurança
- relatórios contratados
- operação da rede

Nunca monitoramos conteúdo de navegação, conversas, mensagens, senhas ou arquivos.
Nunca acessamos dispositivos pessoais.
Nunca compartilhamos dados sem autorização legal.

7. CONTROLES OPERACIONAIS
A CDAtech mantém:
- backups seguros
- controle de acessos baseado em função (RBAC)
- credenciais únicas para administradores
- autenticação multifator
- logs de auditoria
- documentação operacional
- procedimentos de resposta a incidentes

8. RESPONSABILIDADE TÉCNICA
Toda a operação técnica, segurança, políticas de rede e auditorias são conduzidas exclusivamente pelo especialista:

Moacir Havlock
Especialista em Redes, Segurança e Conectividade para Grandes Eventos
DPO – encarregado de proteção de dados
E-mail: moacir@havlock.com.br

Nenhuma alteração de segurança, permissão de acesso, liberação ou ajuste de política é feita sem sua aprovação direta.

9. RESPONSABILIDADE DO USUÁRIO

Espera-se que os usuários:

- Utilizem senhas seguras
- Não compartilhem credenciais
- Não tentem realizar ataques ou scans
- Não utilizem a rede para fins ilegais

Atividades ilícitas são monitoradas, registradas e podem ser encaminhadas às autoridades.

10. COMUNICAÇÃO DE INCIDENTES

Incidentes de segurança podem ser comunicados diretamente ao DPO via:

- moacir@havlock.com.br

Toda comunicação é tratada com urgência e prioridade máxima.

11. ATUALIZAÇÕES DA POLÍTICA

Esta política pode ser atualizada para refletir mudanças técnicas, legais ou processuais.
A versão vigente estará sempre disponível no site da WiFi no Evento.

Concórdia – SC 01 de dezembro de 2025

_____

Luis Filipe Battistella
CDAtech/WiFi no Evento

_____

Moacir Havlock
Havlock Consultoria em TI