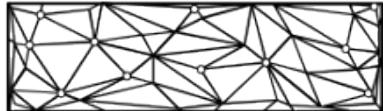


CryptoRave2017 | 5 e 6 de maio



24 horas de atividades sobre segurança, criptografia, hacking, anonimato, privacidade e liberdade na rede

## **CryptoRave**

Inspirada no movimento das CryptoParties – eventos para pessoas comuns aprenderem a usar criptografia forte -, a CryptoRave surgiu no Brasil como um esforço coletivo para difundir os conceitos, a cultura e as ferramentas relacionadas à privacidade, segurança e liberdade na Internet. Chegando a sua quarta edição em 2017, a CryptoRave se consolidou como o maior evento aberto e gratuito deste tipo no mundo, justamente para ampliar o público que discute estes temas.

O evento conta com palestras, debates e oficinas para aprofundar e qualificar o debate sobre a proteção da privacidade na Internet como um direito e fundamento essencial à democracia. Ao final de 24 horas de atividades, uma grande festa: a Rave.

O evento é organizado por Actantes, Encripta Tudo, Escola de Ativismo, Intervozes, Saravá, ativistas e hackers independentes. Em comum, a defesa do direito à privacidade e do desenvolvimento de tecnologias de autodefesa em meio ao cenário de coleta massiva de dados.

## **Autodefesa**

No espírito de compartilhar conhecimento e disseminar informações sobre privacidade, segurança e auto-defesa diante da vigilância massiva de Estados e empresas, a CryptoRave fez o esforço de, a partir do Guia de Autodefesa Digital produzir um mini-Guia introdutório de sobrevivência e autodefesa.

O caminho da autodefesa é proposto por consideramos que as pessoas devem ser responsáveis por sua própria segurança, não acreditamos em soluções prontas e sim na construção de uma cultura coletiva de segurança.

Para saber mais sobre como se defender, acesse o Guia completo em: <https://autodefesa.fluxo.info/>

Leia, use, passe pra frente o conhecimento!

**Sem privacidade não há democracia**

CryptoRave 2017 | <https://cryptorave.org>



## Autodefesa digital

Capacidade de uma pessoa ou grupo se proteger por conta própria de ameaças na comunicação eletrônica.

Por quê? A vigilância hoje é feita automaticamente e em larga escala: as pessoas são monitoradas mesmo que não sejam alvos específicos.

**A seguir um roteiro inicial ajudar você a se proteger e tomar escolhas conscientes! Este também é um convite para que você se aprofunde mais no assunto.**

### Os Princípios Básicos:

1. **Segurança:** toda prática que nos ajuda a agir ao reconhecer e reduzir riscos.
2. **Paranoia:** é deixar de agir por conta de qualquer risco, real ou imaginário.
3. **Privacidade:** conjunto de informações que queremos proteger.
4. **Conforto:** quanto mais confortável e fácil for uma prática de segurança, mais chance ela tem de ser adotada. Cuidado com práticas super complicadas!
5. **Redução de danos:** adote procedimentos de segurança aos poucos, reduzindo os danos de forma sustentável, ao invés de tentar mudanças radicais que não sejam duradouras. Devagar e sempre!
6. **Economia:** procure adotar as práticas de segurança que sejam mais eficazes e menos custosas aos riscos que sejam mais prováveis! Uma boa segurança eleva o custo de alguém te atacar sem que você tenha um custo tão alto para se defender.
7. **Simplicidade:** não compleique suas práticas desnecessariamente. A complexidade desnecessária pode criar falhas na segurança!
8. **Níveis:** uma boa segurança está presente em todos os níveis das tecnologias de comunicação, desde a segurança física dos dispositivos, passando pelos sistemas operacionais, pelos aplicativos e pelos protocolos de comunicação. O comprometimento de um dos níveis compromete no mínimo a segurança de todos os níveis superiores.
9. **Compartimentalização:** é a prática de segurança de isolar informações de acordo com a sua importância e necessidade. Por exemplo, falar com uma pessoa apenas o necessário para uma dada ação e manter algumas informações em círculos restritos de acesso.
10. **Obscuridade:** assuma que o inimigo conhece todas as suas defesas, mesmo que você não saiba se isso é verdade ou não. Isso vai te

ajudar a contar apenas com a eficácia das suas defesas, e não com o fato dela ser ou não ser conhecida.

11. **Abertura:** busque sempre usar hardware, software e protocolos livres e abertos, porque eles podem ser analisados publicamente, o que facilita a correção de falhas de segurança. Mas cuidado, não assuma que todo o software e hardware livre é seguro e livre de falhas. Liberdade e abertura tecnológica são condições necessárias para a segurança, mas não são condições suficientes para a segurança.
12. **Resiliência:** é a capacidade de resistir e se recuperar de ataques. Se as falhas não forem em pontos críticos, é possível se recuperar. Assim, é importante reduzir os pontos críticos de falha.
13. **Autoconsciência:** cultive seu senso crítico e não deixe que as práticas de segurança tirem a sua naturalidade de agir ao tornar você uma pessoa robotizada.



## Segurança da Informação:

A segurança da informação é dividida em algumas propriedades:

1. **Confidencialidade:** é a garantia de que comunicação apenas poderá ser interpretada pelas partes envolvidas, isto é, mesmo havendo interceptação por terceiros, o conteúdo da comunicação estará protegido. Isso significa que, numa comunicação entre você e outra pessoa, haverá confidencialidade se apenas vocês tiverem acesso ao conteúdo da comunicação.
2. **Integridade:** é a garantia de que o conteúdo da comunicação não foi adulterado por terceiros. Ou seja, na comunicação entre você e outra pessoa, vocês conseguem identificar se alguém alterou o conteúdo das mensagens.
3. **Disponibilidade:** é a garantia de que o sistema de comunicação estará acessível sempre que necessário. Este é um requisito de segurança porque a falta de comunicação pode ser muito prejudicial.
4. **Autenticidade:** garante que cada uma das partes possa verificar se está de fato se comunicando com quem pensa estar se comunicando, isto é, a garantia de que não há um impostor do outro lado da comunicação.
5. **Não-repúdio:** garante que as partes envolvidas na comunicação não possam negar ter participado da comunicação. Esta propriedade é desejada em sistemas nos quais haja um controle sobre quem realizou determinados tipos de operações.
6. **Negação plausível:** o oposto do não-repúdio é a negação plausível,

no caso onde não é possível determinar com certeza se determinada pessoa participou da comunicação.

7. **Anonimato:** é garantia de que as partes envolvidas na comunicação não possam ser identificadas.

Nem sempre os sistemas satisfazem todas essas propriedades, seja intencionalmente ou não. É importante observar o que cada sistema oferece em termos dessas propriedades e se elas estão bem implementadas no sistema.

Por exemplo, alguns sistemas foram criados para possuir a propriedade do não-repúdio, enquanto outros são baseados na negação plausível.

Em muitas situações, é possível combinar diversos sistemas que ofereçam propriedades distintas de segurança da informação para obter o máximo de propriedades possíveis.



## Limites da segurança

Viver é perigoso! Mas o que seria viver sem arriscar?

Segurança tem limites e faz parte de uma atitude segura saber quais são eles. Os principais são:

1. **Incompletude:** não existe segurança total ou sistema infalível. Todo sistema possui falhas.
2. **Ceticismo:** é possível descobrir se sua segurança está sendo comprometida, mas isso nem sempre acontece. Pode ser que sua segurança esteja sendo comprometida sem que você saiba. Adote um ceticismo saudável para não ter ilusões sobre a sua segurança.
3. **Malícia:** nem sempre uma falha é resultado de um ataque intencional. Às vezes a comunicação tem problemas por falta de qualidade e não porque alguém esteja te atacando. Muitas vezes é difícil saber se você está sendo atacada/o ou se está sofrendo apenas uma falha de funcionamento num dispositivo. É sempre bom estar alerta e não baixar a guarda, mas você não precisa assumir logo de cara que está sendo atacada/o sempre que houver falha. Menos paranoia, mais senso crítico e intuição!
4. **Preparação:** prepare-se para a possibilidade da suas práticas seguras falharem. Quando a casa cair, o que você vai fazer? Se preparar para isso também é uma prática segura!



## Checklist

Mais do que sair adotando práticas e ferramentas de segurança, é importante que você tenha uma noção do todo e também das partes, ou seja, que você organize suas práticas de segurança num todo consistente.

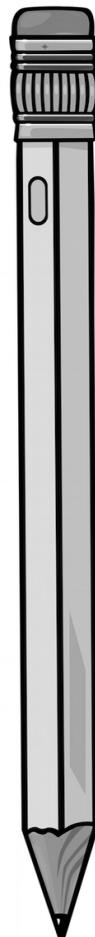
Uma maneira fácil de fazer isso é manter um Checklist de Segurança:

1. Faça uma lista das suas atividades. Como cada uma delas funciona? Elas dependem de algum dispositivo tecnológico? Como eles funcionam em linhas gerais? Pesquise!
2. Quais são as ameaças envolvidas nessas suas atividades? Quem poderia te atacar? Como os dispositivos tecnológicos poderiam falhar? Pesquise e use a sua imaginação!
3. A partir do conhecimento reunido, como você poderia se proteger?

Existem diversos guias práticos sobre como se defender.

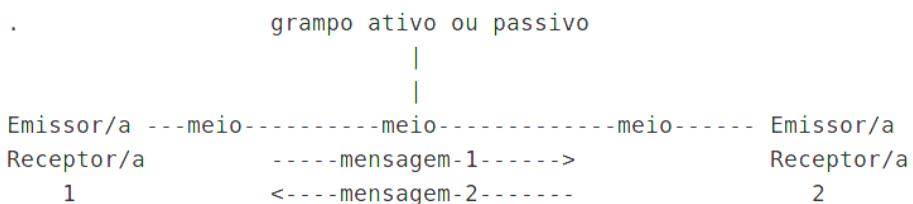
Por fim, **faça escolhas**:

- Comece pequeno e vá aos poucos. Você é capaz!
- Priorize as ameaças mais prováveis e as defesas que estejam ao alcance da sua capacidade. Cada pessoa tem seu ritmo.
- Segurança não é um fetiche: não adote uma prática só porque ela está na moda ou é considerada chique, mas sim se ela é útil para você.



## Comunicação Digital

Nosso foco aqui é comunicação digital! Então vamos começar com nosso desenho esquemático da Teoria da Comunicação Hacker:



Nesse desenho, duas partes envolvidas numa comunicação trocam mensagens entre si através de um meio que assumimos estar grampeado por padrão!

Ele não precisa estar necessariamente grampeado, mas se assumirmos que ele está, nós já estaremos nos preparando para as situações em que ele esteja!

Os ataques fundamentais da vigilância das comunicações são:

1. Interceptação de Dados: é a escuta do conteúdo da comunicação. Pode ser passiva – apenas grava a comunicação – ou ativa – quando também interfere na comunicação, alterando mensagens.
2. Interceptação de Metadados: quando apenas as informações básicas da comunicação são gravadas. Quem fala com quem, quando, onde, por quanto tempo, etc, sem que o conteúdo das mensagens seja obtido necessariamente.

É importante saber que algumas práticas de segurança protegem apenas os dados, enquanto outras protegem apenas os metadados da comunicação. Também existem práticas que protegem ambos!

Lembre-se que a vigilância é feita não apenas pelos governos, mas também por empresas.



## Criptografia

Usamos criptografia para nos defender dos ataques à comunicação digital.

Ela codifica dados e/ou metadados para que a informação possua um ou mais critérios de segurança como confidencialidade, integridade e autenticidade.

Em sua aplicação mais básica, a criptografia é a técnica de codificar mensagens de tal modo que apenas quem possuir o segredo de como decodificá-las pode acessar seu conteúdo original.

Essas e outras propriedades da segurança da informação podem ser obtidas juntas ou separadas dependendo do sistema criptográfico em uso.

Hoje é essencial que meios de comunicação possuam algum tipo de criptografia, sendo essa uma condição básica para que resistam a ataques informacionais.

Para ser eficaz, a criptografia precisa usar padrões bem estabelecidos e ser bem implementada, do contrário ela só traz ilusão de segurança. Também é importante que a criptografia seja de ponta-a-ponta, isto é, que seja realizada integralmente nos dispositivos de comunicação das pessoas e não em dispositivos intermediários e que estejam fora do nosso controle.



## Senhas

Para usar sistemas de comunicação com mais segurança é importante saber o básico e essencial sobre senhas.

Para ter acesso a determinados sistemas ou lugares, pode ser necessário fornecer uma prova de acesso para que ocorra uma **autenticação**, isto é, uma permissão de acesso.

Existem vários tipos de autenticação:

1. A autenticação pode ser baseada em algo que você carrega: por exemplo um cartão de crédito, um crachá ou documento de identificação.
2. A autenticação pode ser baseada em algo que só você ou um grupo restrito de pessoas sabe. Chamamos essa informação de **senha**.
3. Ela também pode se basear em alguma característica física sua e nesta caso estamos falando de **biometria**.

Aqui trataremos apenas sobre senhas, que é a forma de autenticação mais utilizada na comunicação digital. Biometria pode ser forjada e algo que você carrega no bolso pode ser roubado. Mas extrair uma senha da sua mente já envolve mais trabalho. Daí o poder das senhas!

Boas senhas possuem as seguintes características:

1. **Memorizável**: uma senha muito difícil de lembrar pode levar ao seu esquecimento e ser difícil de digitar.  
Já uma senha muito fácil de lembrar também pode ser muito fácil de alguém descobrir. Senhas muito fáceis em geral também tem um tamanho pequeno, então pense num tamanho mínimo e memorizável quando criar sua senha.
2. **Difícil de descobrir**: quanto mais difícil de descobri-la, melhor. Mas isso pode acarretar numa complexidade da senha que a torna difícil de lembrar.
3. **Pouco ou não compartilhada**: se você usa a senha para uma coisa, e uma única coisa apenas, é mais difícil dela ser descoberta. Quanto mais compartilhada, maior o risco, pois a superfície de ataque à senha aumenta.

Esta característica vem diretamente do princípio da compartmentalização: se uma senha for comprometida, o dano estaria restrito apenas a um ou poucos sistemas.

Uma senha roubada pode ser usada como tentativa para invadir outros sistemas. Se você usa a mesma senha para mais de um sistema e ela for roubada, trate logo de mudar a senha em todos os sistemas.



## Computadores

O computador se transformou no elemento básico da comunicação digital.

Existem muitas falhas nos computadores em todos os níveis: no hardware, no sistema operacional e nos programas utilizados, assim como muitas formas de se defender.

Medidas básicas de segurança para computadores incluem:

- Usar software livre, como o sistema operacional Debian GNU/Linux.
- Usar criptografia de armazenamento.
- Manter o sistema sempre atualizado.

Consulte documentações específicas para mais detalhes :)



## Telefones

Os smartphones são uma catástrofe em termos de segurança e privacidade:

1. Seu funcionamento é baseado no rastreamento do aparelho, ou seja, todo telefone móvel é um dispositivo de rastreamento.
2. Existem problemas no hardware dos telefones que permitem acesso especial pelas operadoras de telefonia ou atacantes especializados.
3. O smartphone é também um computador, possuindo diversas das vulnerabilidades existentes em computadores.
4. O smartphone foi feito intencionalmente para ser um coletor automáticos de informações. Essas informações seguem para diversas empresas que a utilizam de forma estratégica para levarem vantagem em relação a toda a sociedade. Muitas dessas informações também acabam nas mãos dos governos e outras organizações.

É muito difícil usar um telefone de forma segura pois a arquitetura dos smartphones joga o tempo todo contra a segurança e a privacidade. Aqui não há espaço para uma análise detalhada então deixamos apenas as dicas mais básicas:

1. Mantenha o sistema do seu telefone sempre atualizado.
2. Preste atenção nas permissões solicitadas por cada aplicativo que você instalar.  
Repare que aplicativos maliciosos podem encontrar maneiras de burlar restrições no sistema.
3. Quanto menos aplicativos você usar, melhor. Pense no que é essencial para você. Mesmo aplicativos que pareçam ser inofensivos podem causar danos.

4. Dê preferência para softwares livres ou abertos. Além da loja de aplicativos padrão do seu telefone, você pode instalar lojas que oferecem apenas softwares livres.

Sempre procure uma opção livre e aberta antes de buscar por um software fechado.

5. Quando precisar ter uma conversa sigilosa com alguém, combine com a pessoa para que vocês deixem seus telefones em casa antes de se encontrarem. Isso evita rastreamento e gravação de conversas via smartphone.

A medida mais simples e eficaz é não usar telefone, mas hoje em dia está cada vez mais difícil viver sem ele por conta de imposições sociais. Assim, pode ser necessário fazer um uso estratégico dessa tecnologia.



## Segurança na Rede

Qualquer informação que enviamos na internet está sujeita à vigilância.

É fácil nos conscientizarmos de quais informações enviamos voluntariamente, porém é mais difícil perceber informações adicionais, ou metadados, que são enviados automaticamente pelos softwares e serviços que utilizamos.

### Quais são as informações que nos identificam e rastreiam nossos hábitos?

Rastreadores embarcados nos sites, como coletores de estatísticas e botões do tipo “curtir” conseguem estimar se estamos autenticados na respectiva rede social, qual o nosso login, etc.

Uma única página da web pode vir embutida com rastreadores de diversos serviços.

Este é o grande resumo que vale para redes sociais, mensageria, dados de formulário, informações de buscas, etc: Basicamente **TUDO** o que você envia na internet pode ser guardado indefinidamente, integrado a bancos de dados ou vazado.

E bastam poucas dessas informações para que seja possível nos identificar unicamente.

Como podemos nos defender de uma situação em que qualquer interação pode ser registrada e utilizada indefinidamente? Existe uma saída para a segurança da informação ou este é o fim da privacidade?

Estas são boas perguntas. A história dirá. Por hora, temos algumas medidas de segurança possíveis para melhorar um pouco nossa situação.

1. Garantir a segurança da informação básica: a comunicação criptografada usando **HTTPS** é a forma básica de se transferir

informações na web.

O uso do HTTPS nos dá mais garantias de que estamos acessando o sítio legítimo e não uma versão falsa. Também garante que a comunicação não poderá ser interpretada ou adulterada por interceptadores.

O uso do HTTPS depende da oferta deste pelo site ou serviço que você queira acessar. Um sítio que use HTTPS terá o seu endereço no navegador começando por **https://**, como por exemplo **https://wikipedia.org**.

O fato do HTTPS estar disponível em um site não implica necessariamente que a conexão é segura. O HTTPS possui vários problemas, como a dependência da certificação criptográfica feita por terceiros que podem ser invadidos ou serem compelidos a emitir certificações falsas.

Ainda, o HTTPS pode estar mal implementado nos sites.

2. Usar logins e serviços somente quando necessário: você precisa estar autenticado(a) o tempo todo nas redes sociais? Quanto menos você usá-las, menos irão te rastrear.
3. Você pode utilizar um navegador especial feito para proteger a sua privacidade.

Recomendamos que você utilize o **Tor Browser** no seu computador e, no seu smartphone, o **Orfox** juntamente com o **Orbot**.

Ambos os softwares utilizam a rede **Tor**, que é uma plataforma de navegação mais anônima. Ela utiliza criptografia e uma grande rede de computadores distribuídos pela internet, que dificulta muito a localização dos usuários que estão navegando.

O Tor Browser é um navegador que usa a rede **Tor** em todas as suas conexões. Isso significa que ao navegar usando o Tor Browser você já estará, por padrão, dificultando sua localização na internet.

Mas **ATENÇÃO**: certifique-se de sempre usar conexão HTTPS ao acessar qualquer site usando o Tor Browser. Do contrário, você estará muito mais suscetível a ataques de interceptação e de site falso. O Tor Browser também possui uma série de modificações de segurança para que a sua navegação fique mais segura. Já o Orbot permite que seus aplicativos no smartphone utilizem a rede Tor.

4. Procure usar serviços que respeitem a sua privacidade e que não façam dinheiro a partir da coleta das suas informações.



## Mensageria

A decisão de quais comunicadores instantâneos utilizar é muito importante. Aqui seguem dicas para que você tenha condições de escolher por conta própria:

- 1. A aplicação de mensageria é bem estabelecida?** Existem inúmeros aplicativos para comunicação instantânea, muitos deles afirmando inclusive serem seguros quando não são. O primeiro fator de insegurança pode ser um aplicativo que em si é inseguro.
- 2. No caso do aplicativo oferecer criptografia, ela é de ponto a ponto?** Ou o conteúdo das mensagens pode ser acessado pelo serviço de mensageria?  
Pode ser importante observar também se a criptografia de ponta a ponta oferece negação plausível e a possibilidade de identificar chaves a usuários.  
No geral, a criptografia do aplicativo é bem implementada?  
A criptografia opera também nos metadados?  
Nem sempre é fácil responder essas perguntas e por isso é importante ficar de olho nos aplicativos recomendados pela comunidade de segurança.

### 3. Como é feito o login na aplicação?

Aplicativos que funcionam no computador, em geral, possuem autenticação com senha. Mas, no caso dos comunicadores de celular, a criação de contas envolve a checagem com número de telefone como identificador global de usuários.

Isso tem vários problemas. O número de telefone não é um dado anônimo e nem propriedade do usuário, mas sim da companhia telefônica. Além disso, se mal implementada, essa confirmação pode ser burlada por atacantes para roubar sua conta ou espionarem a sua comunicação.

### 4. Onde ficam armazenadas as mensagens?

É importante saber se as mensagens ainda não entregues ficam armazenadas no servidor sem criptografia. E, se depois de entregues, ficam armazenadas no dispositivo do usuário também sem criptografia.



## Softwares Recomendados

### No smartphone:

- Signal Messenger para comunicação instantânea.
- Orbot e Orfox para navegação anônima.
- No Android, use a central de aplicativos livres F-Droid.
- Se possível, utilize um sistema operacional livre como o LineageOS.

### No computador:

- Adote um sistema operacional livre, como o Debian GNU/Linux.
- Use o Tor Browser Bundle para navegação na web com mais anonimato.
- Para situações críticas, use o Tails, um sistema operacional livre e mais seguro.

## Referências

- Guia de Autodefesa Digital - <https://autodefesa.fluxo.info>
- Tem boi na linha? Guia prático de combate à vigilância na internet - <https://temboinalinha.org>
- A Criptografia Funciona - Como Proteger Sua Privacidade na Era da Vigilância em Massa - <https://we.riseup.net/deriva/a-criptografia-funciona-como-proteger+260170>
- Security in a Box - Ferramentas de Segurança Digital para todas as pessoas - <https://securityinabox.org/pt/>
- PRISM Break - <https://prism-break.org/pt/>
- Guia de Protestos - <https://protestos.org>

Este conteúdo está disponível sob a licença Creative Commons — Attribution-ShareAlike 3.0 Unported — CC BY-SA 3.0  
<https://creativecommons.org/licenses/by-sa/3.0/>

# Programação da CryptoRave 2017

## GÊNERO

Título	Responsáveis	Data, Hora e Local
<b>An Averaging Mirror (Um espelho normal)</b> Nossa crescente dependência a tecnologia pessoal está ligada com a crescente opacidade dos dispositivos que nós usamos.	Zeesy Powers	<b>Dia:</b> 05/05/2017 <b>Hora:</b> 22:00 <b>Room:</b> Performances
<b>Cientistes, artistes, precáries, programadoras, hacktivistes, riotgrrrls: Hackfeminista na América Latina</b> A proposta desta oficina é reunir mulheres e pessoas trans que conheçam ou ou estejam envolvidas em projetos ciberfeministas.	Steffania Paola	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 16:30 <b>Room:</b> Ada Lovelace
<b>(Cyber) espaços seguros</b> Nesta oficina explicaremos conceitos básicos de redes usando linguagem e metodologia focada no público feminino.	Carl	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 15:20 <b>Room:</b> Ada Lovelace
<b>De volta ao Cyberfeminismo</b> A proposta dessa mesa é um debate através de um olhar Ciberfeminista sobre as dificuldades encontradas pelas mulheres nos estudos e no mercado de trabalho de TI.	Jussara Oliveira	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 13:00 <b>Room:</b> Ada Lovelace
<b>Mnemosine</b> Criação de um jogo da memória que resgate e destaque o nome de mulheres cientistas no passado e na contemporaneidade.	Daniela Araújo	<b>Dia:</b> 05/05/2017 <b>Hora:</b> 23:50 <b>Room:</b> Ian Murdock
<b>Outro pornô é possível: Anonimato e privacidade para nossa Intimidade</b> Neste workshop, abordaremos a importância do anonimato para nossa liberdade de uma perspectiva feminista.	fer	<b>Dia:</b> 05/05/2017 <b>Hora:</b> 23:50 <b>Room:</b> Ada Lovelace
<b>SexHacking</b> O encontro entre tecnologia e sexualidade pode gerar resultados surpreendentes, ampliando a percepção do corpo humano e suas possibilidades.	Rita Wu	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 02:00 <b>Room:</b> Ada Lovelace

Título	Responsáveis	Data, Hora e Local
<b>SexHacking #5</b> O workshop consiste na aproximação entre sexo e tecnologia, com o objetivo de criar um dispositivo wearable para o prazer.	Rita Wu	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 02:25 <b>Room:</b> Ada Lovelace
<b>Um pouquim sobre Ada, condessa de Lovelace</b> Ada August Byron King foi a pioneira da lógica de programação, tendo inventado alguns dos conceitos utilizados até hoje quando se cria programas.	facontí	<b>Dia:</b> 05/05/2017 <b>Hora:</b> 22:40 <b>Room:</b> Ada Lovelace
<b>Violência cibernética - Como atacar e se manter segur@</b> Quando nos posicionamos como ativistas - seja com feminismo, seja com hackerativismo - o embate é quase impossível de ser evitado.	Val Barros	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 09:00 <b>Room:</b> Ada Lovelace
<b>Violência online, privacidade e anonimato</b> A Coding Rights, uma organização de direitos digitais liderada por mulheres. Como fazer frente aos ataques racistas, sexistas e a repressão política online sem ampliar os poderes de censura e vigilância de Estado e empresas?	rrenno	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 09:30 <b>Room:</b> Ada Lovelace

## SEGURANÇA

Título	Responsáveis	Data, Hora e Local
<b>A NSA e o fim da privacidade</b> Nossa cultura de super exposição online e as capacidades de vigilantismo tecnológico decretaram o fim da privacidade na era da informação.	Anchises	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 02:00 <b>Room:</b> Alan Turing
<b>A receita do FBI para atacar a rede TOR</b> A palestra tem o objetivo de usar dados técnicos sobre um fato histórico como um microcosmo para analisar a maneira que as operações policiais contra dark markets vem ocorrendo e possivelmente contribuir para o debate técnico e moral sobre o tema.	Carlos Cabral	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 17:40 <b>Room:</b> Edward Snowden
<b>Ativistas e movimentos sociais na internet</b> Apresentação de algumas ferramentas e programas que podem ser usados para organização, articulação e comunicação segura, com um foco especial em movimentos sociais e ativistas.	Raquissa e Jack	<b>Dia:</b> 05/05/2017 <b>Hora:</b> 22:40 <b>Room:</b> Aaron Swartz

Título	Responsáveis	Data, Hora e Local
<b>Autodefesa Digital e Educação em Segurança</b> Lançamento do Curso Online de Autodefesa Digital e da nova versão do Manual de Segurança.	rhatto	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 03:00 <b>Room:</b> Edward Snowden
<b>Bigdata e saúde</b> Apresentação da palestra da Goa sobre o mestrado dela que estuda big data no SUS, como tratar dos dados cuidando da privacidade.	goa	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 01:00 <b>Room:</b> Ada Lovelace
<b>Capitalismo de Vigilância e a ameaça a Direitos Humanos na Era Pós-Snowden</b> As revelações de Edward Snowden desempenharam importante papel ao lançar luz sobre as práticas de vigilantismo em massa.	Núcleo de Estudos em Tecnologia e Sociedade - NETS/USP	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 12:00 <b>Room:</b> Edward Snowden
<b>Computação Forense</b> No momento político turbulento que estamos passando, apresentarei as etapas básicas que constituem uma investigação computacional forense.	M4TT0S	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 16:30 <b>Room:</b> Alan Turing
<b>Conhecendo o Qubes OS</b> Uma conversa sobre o Qubes OS, considerado um dos sistemas operacionais atuais mais seguros, mas que também busca poder ser usado por qualquer pessoa.	Andrés Martano	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 14:10 <b>Room:</b> Alan Turing
<b>Criando Sistemas de Autenticação Seguros</b> Mostrar os desafios de construir um sistema de Autenticação Simples mas Seguro usando algumas técnicas de criptografia para salvar de maneira segura os dados dos usuários.	Dann Luciano	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 13:00 <b>Room:</b> Edward Snowden
<b>Design Sombrio: Como a UX de Grandes Empresas Reduz a Privacidade dos Usuários</b> Os padrões sombrios do UX Design se tornaram uma prática comum de grandes... Vou mostrar aqui alguns casos reportados sobre grandes empresas, destacando o que foi feito, qual comportamento humano foi explorado e qual era o objetivo esperado com aquela interface.	Patrícia Estevão	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 12:25 <b>Room:</b> Alan Turing
<b>Dispositivos móveis e privacidade - antivigilância</b> Elementos culturais do uso do celular e seus riscos à privacidade, invasões à privacidade e soluções e técnicas de	rrenno	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 18:50 <b>Room:</b> Ada

Título	Responsáveis	Data, Hora e Local
mobilização e resposta por parte do cidadão.		Lovelace
<b>Distribuição MarrecoBSD</b> A nova distribuição operacional livre baseada em Kernel BSD, tem como seu princípio a reformulação das interatividades desempenhadas pelos usuários.	Matheus H. Silva	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 18:50 <b>Room:</b> Alan Turing
<b>Explicando segurança e privacidade com Wireshark</b> Como o Wireshark pode ser utilizado para demonstrar na prática conceitos relacionados a segurança e privacidade.	Euler Neto	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 17:40 <b>Room:</b> Alan Turing
<b>Festival do Anonimato</b> Terá como foco ajudar pessoas que estão em foco no processo de vigilância de movimentos sociais, ativistas de direitos humanos e jornalistas livres.	Gomex	<b>Dia:</b> 05/05/2017 <b>Hora:</b> 22:40 <b>Room:</b> Install Fest
<b>GNU/Linux para noobs</b> Aprenda a filosofia e conceitos de GNU/Linux e por quê tão importante utilizá-lo no contexto de vigilância em massa!	Daniela Morais	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 16:30 <b>Room:</b> Install Fest
<b>Linux 100% Encriptado - Uma abordagem prática</b> Como instalar Linux "from scratch", com todas as partições de disco encriptadas.	Fernão Vellozo	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 12:00 <b>Room:</b> Install Fest
<b>Minha experiência como operador de um relay Tor</b> Como escolher um provedor, tipos de relays, implicações legais, clico de vida de um relay, etc.	Augusto Amaral	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 01:00 <b>Room:</b> Aaron Swartz
<b>Mini guia para se manter mais "seguro" na Internet</b> Este pequeno guia irá nortear a sua mudança comportamental para navegar de forma mais segura na Internet.	corvolino	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 09:00 <b>Room:</b> Install Fest
<b>Navegação com privacidade para iniciantes</b> Oficina voltada para iniciantes no tema. Nessa oficina você vai conhecer um pouco de como funciona a navegação na internet e quais são as ferramentas e técnicas que se podem usar para navegar com mais privacidade.	Leo Germani	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 09:00 <b>Room:</b> Aaron Swartz
<b>Oficina de senhas mais seguras</b> Oficina ensinando dicas para criar uma senha diferente para	Memeco	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 15:20

Título	Responsáveis	Data, Hora e Local
cada site + dicas para fortalecerem essas senhas.		<b>Room:</b> Install Fest
<b>OONI (Open Observatory of Network Interference)</b> A free software, global observation network for detecting censorship, surveillance and traffic manipulation on the internet.	Vasilis	<b>Dia:</b> 05/05/2017 <b>Hora:</b> 22:40 <b>Room:</b> Chelsea Manning
<b>OpenBSD pra Viver</b> Para aumentar as chances da privacidade no Desktop dos usuários, apresentamos o OpenBSD .	Alexandre Deckleva	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 02:00 <b>Room:</b> Edward Snowden
<b>Privacy Enhancing Design</b> Essa conversa é pra mostrar que privacidade e segurança não é só pra hacker, é pra qualquer um e design pode ajudar.	Virginia Stefanello	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 12:00 <b>Room:</b> Alan Turing
<b>Próximos passos do Securegen</b> O que falta para termos uma distribuição livre, segura e amigável para celular.	Márcio M. Ribeiro	<b>Dia:</b> 05/05/2017 <b>Hora:</b> 23:50 <b>Room:</b> Alan Turing
<b>Realmente nada a esconder?</b> Orientações sobre privacidade para pessoas que estão começando a se preocupar com suas informações pessoais na internet.	Thais, Camilla e Tayane	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 17:40 <b>Room:</b> Aaron Swartz
<b>Reforma agrária do ciberespaço</b> Uma introdução a segurança digital para sites com o objetivo de incentivar a existência de espaços fora dos "jardins murados" dos grandes portais.	Carl	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 12:00 <b>Room:</b> Chelsea Manning
<b>Sem título (informação sigilosa)</b> Tanto o título quanto o conteúdo da performance são secretos.	Secretas	<b>Dia:</b> 07/05/2017 <b>Hora:</b> 00:00 <b>Room:</b> Rave AlJaniah - Térreo
<b>Técnicas de Espionagem e Contra Inteligência</b> Apresentação sobre como os Crackers, agências de inteligência e governos utilizam técnicas e ferramentas simples para obter informações sobre os alvos e como se prevenir dessa vigilância.	Emmanoel Lourenço	<b>Dia:</b> 05/05/2017 <b>Hora:</b> 22:40 <b>Room:</b> Ian Murdock

## CRIPTOGRAFIA

Título	Responsáveis	Data, Hora e Local
<b>As propostas de criptografia dos engenheiros da Internet</b> Apresentação da proposta política do Internet Engineering Task Force para segurança de dados e criptografia	Antonio Moreiras	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 16:30 <b>Room:</b> Chelsea Manning
<b>Criptografando sua rede com a Raspi!</b> Vamos instalar um cliente VPN em um nanocomputador Raspberry Pi, e aprender como configurá-lo para criptografar todo o tráfego de uma rede local.	bruno vianna	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 01:00 <b>Room:</b> Alan Turing
<b>Criptografia com Automatos Celulares</b> Será realizada uma apresentação bastante visual e interativa sobre criptografia.	Daniel Carvalho	<b>Dia:</b> 05/05/2017 <b>Hora:</b> 23:50 <b>Room:</b> Edward Snowden
<b>Deixem a criptografia em paz!</b> A ideia é desmistificar o debate atual em torno da criptografia e propor alternativas menos intrusivas para fins de investigação.	Diego F. Aranha	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 16:30 <b>Room:</b> Edward Snowden
<b>Dúvidas por aqui: PitStop da privacidade</b> Tem dúvidas? Nós temos as respostas. Chega mais, aqui na nossa mesa.	Tania S.	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 13:50 <b>Room:</b> Install Fest
<b>Helios Voting</b> Como funciona um sistema sistema de votação online? Ele é seguro? Entenda um pouco mais dessa ferramenta cada vez mais importante nos dias de hoje.	João Moreno Giulia Vieira	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 02:00 <b>Room:</b> Chelsea Manning
<b>O elo mais fraco da nossa segurança: S&amp;nh5s</b> Entenda o que são, como criar e gerenciar senhas fortes.	caioau	<b>Dia:</b> 05/05/2017 <b>Hora:</b> 22:40 <b>Room:</b> Alan Turing
<b>Oficina de instalação do provedor LEAP</b> Essa sessão ajudará você respondendo qualquer dúvida durante a instalação do provedor LEAP numa máquina local vagrant ou em servidores remotos.	Varac	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 01:00 <b>Room:</b> Install Fest

Título	Responsáveis	Data, Hora e Local
<b>Privacidade no Mundo Pós-quântico</b> Será apresentado o modelo de segurança atual dos protocolos criptográficos, como eles ficariam vulneráveis a um ataque quântico e quais são as frentes de pesquisa em andamento para evitar que isso ocorra.	Diego Mariano	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 15:20 <b>Room:</b> Alan Turing
<b>Se Encriptando em 30m</b> Essa palestra pretende mostrar de forma rápida e prática como encriptar o disco rígido, discos removíveis e arquivos.	Erick Emiliano	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 13:00 <b>Room:</b> Alan Turing
<b>Tor meetup</b> Um encontro dos usuários Tor, desenvolvedores, operadores de relays e todas as pessoas que querem se juntar.	ilv Vasilis	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 12:00 <b>Room:</b> Laje
<b>Tor relays (en América Latina)</b> O objetivo desta apresentação é motivar mais voluntários da região para contribuir com a diversidade da rede Tor.	ilv	<b>Dia:</b> 05/05/2017 <b>Hora:</b> 23:50 <b>Room:</b> Chelsea Manning

## POLÍTICA

Título	Responsáveis	Data, Hora e Local
<b>5 tópicos sobre a Saúde da Internet no Mundo</b> Entender como as pessoas percebem e interagem com a Internet fundamental para saber o quanto saudável a Internet está e quais são as oportunidades que podem ser geradas a partir dela.	Geraldo Barros	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 09:00 <b>Room:</b> Chelsea Manning
<b>"Assoprando o apito": o papel do jornalismo investigativo num mundo vigiado</b>	Joana Varon Andrew Fishman	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 14:10 <b>Room:</b> Edward Snowden
<b>Ativismo alimentar sob ataque</b> Esta atividade será uma roda de discussão sobre o caso de espionagem que ocorreu no México com a ONG El Poder del Consumidor e outros parceiros que trabalham para avançar com políticas públicas em alimentação e nutrição.	Ana Paula Bortoletto	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 13:00 <b>Room:</b> Chelsea Manning

Título	Responsáveis	Data, Hora e Local
<b>Aumento do aparato de vigilância no Brasil</b> Mesa de discussão sobre o avanço do aparato de vigilância no Brasil, considerando novas leis e arcabouço legal, criação de novos órgãos, compra e uso de novos dispositivos de vigilância e casos de abuso e violação de direitos.	amarela	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 15:20 <b>Room:</b> Edward Snowden
<b>Brasil Hostil: como você vai dançar?</b> Mostraremos o cardápio disponível pra parar no xilindró neste Brasil contemporâneo.	rhatto gus	<b>Dia:</b> 05/05/2017 <b>Hora:</b> 23:50 <b>Room:</b> Aaron Swartz
<b>Como os órgãos públicos respondem a pedidos de informação sobre cibersegurança.</b> O propósito desta sessão é apresentar as respostas obtidas para ilustrar o atual cenário da cibersegurança e ciberdefesa brasileiro sob a ótica dos setor público federal	ARTIGO 19	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 15:45 <b>Room:</b> Edward Snowden
<b>CooLab</b> Nossa ideia é propor um modelo autossustentável de criação de redes: os investimentos feitos para infraestrutura são retornados pela comunidade através da exploração da própria rede.	bruno vianna	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 16:45 <b>Room:</b> Laje
<b>Criptografia e Agroecologia</b> A partir da experiência concreta de mulheres agricultoras no Vale do Ribeira, a roda de conversa irá explorar os diálogos entre a criptografia e a agroecologia enquanto alternativas de resistência.	Marcha Mundial das Mulheres	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 14:10 <b>Room:</b> Ada Lovelace
<b>Cripto Guerra Estilo Brazuca</b> As tentativas da justiça brasileira de bloquear serviços de comunicação criptografada ou a postura do TSE em relação às urnas eletrônicas são apenas a ponta do iceberg do despreparo no trato de temas ligados à tecnologia e sociedade.	Anderson Ramos	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 01:00 <b>Room:</b> Edward Snowden
<b>Espionagem no brasil: a estrutura e os alvos.</b> A palestra pretende mostrar a rede de conexões das agências de espionagem no Brasil, sua estrutura e dinâmica.	sergio amadeu	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 13:00 <b>Room:</b> Aaron Swartz
<b>Estudos em Vigilância: tecnopolítica, controle, infraestruturas e formas de vida</b> Pesquisadores da LAVITS (Rede Latino-Americana de Estudos	Henrique Parra	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 17:40

Título	Responsáveis	Data, Hora e Local
em Vigilância, Tecnologia e Sociedade) apresentação do estado da arte em campos específicos dos estudos em vigilância, tecnologia e sociedade.		<b>Room:</b> Chelsea Manning
<b>Free Digital Territories</b> Restricting laws referring topics like data retention, radio lockdown or the telemedia regulations are effecting community WIFI projects in different ways.	pegs	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 14:10 <b>Room:</b> Laje
<b>Infiltração de agentes em manifestações, movimentos sociais e grupos dissidentes</b> Mesa de conversa com ativistas, advogadxs e pesquisadorxs sobre a técnica de infiltração de agentes em manifestações, movimentos sociais e grupos dissidentes, considerando a legalidade das ações e o impacto para os grupos e indivíduos afetados.	escola de ativismo	<b>Dia:</b> 05/05/2017 <b>Hora:</b> 22:40 <b>Room:</b> Edward Snowden
<b>Listatona OONI contra a censura na web</b> A Coding Rights, em parceria com o Open Observatory of Network Interference (OONI) / Tor Project, vai promover um encontro para expandirmos juntas a lista de sites a serem testados no Brasil e em outros países da Latinoamérica pelas sondas do OONI. Se puder, traga seu computador com o Navegador Tor instalado!	Coding Rights Vasilis	<b>Dia:</b> 05/05/2017 <b>Hora:</b> 22:55 <b>Room:</b> Chelsea Manning
<b>Nossa rede, nossas regras - montando redes comunitárias</b> A oficina visa apresentar os principais pontos para planejar e construir uma rede comunitária a partir do relato de uma comunidade que já possui uma rede e o trabalho prévio de organizações que construíram uma metodologia para o cenário de provimento de acesso brasileiro.	ARTIGO 19	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 17:40 <b>Room:</b> Laje
<b>O Projeto Debian quer você!</b> Venha aprender como você pode contribuir com o Projeto Debian mesmo não tendo conhecimento técnico para fazer empacotamento de software.	Paulo Santana	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 14:10 <b>Room:</b> Install Fest
<b>Política e tecnologia na sociedade do controle</b> É uma oficina básica para apresentar os aspectos políticos e tecnológicos da Cultura de Segurança.	Coletivo Mariscotron	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 14:10 <b>Room:</b> Aaron Swartz

Título	Responsáveis	Data, Hora e Local
<b>Privacidade e Relações de Trabalho</b> Debate sobre as formas como as atuais relações de trabalho controlam e registram informações privadas dos trabalhadores.	Infoproletários	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 09:00 <b>Room:</b> Edward Snowden
<b>Privacidade onde importa: Esconda seus bilhões em offshores</b> Como funciona o processo de offshores? Porque é uma desgraça para a justiça, a economia e tudo o que há de bom.	Tiago Fassoni	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 01:00 <b>Room:</b> Chelsea Manning
<b>Subvertendo o capitalismo de vigilância</b> Unir as agendas de privacidade e segurança com projetos econômicos alternativos ao padrão corporativo do Vale do Silício.	Rafael Zanatta	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 13:00 <b>Room:</b> Laje
<b>The Future is Peer-to-Peer</b> Our computers are moving into the cloud. The internet is being centralized. It is turned into a shopping mall where we are tolerated as passive consumers.	Torsten Grote	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 14:10 <b>Room:</b> Chelsea Manning
<b>#TopSacanagem</b> Explicar o funcionamento da Coalizão e dar detalhes do trabalho realizado em Brasília, atualizando o que há de mais perverso rolando na terra da sacanagem estruturada.		<b>Dia:</b> 06/05/2017 <b>Hora:</b> 15:20 <b>Room:</b> Chelsea Manning
<b>Uma crise de identidades: vigilâncias e ameaças às identidades de gênero na internet; o que (não) fazemos e devemos</b> Vemos evidenciar não apenas um tema, mas uma grande crise. De identidades de gênero. De atuações. De mudanças drásticas nas medidas e contramedidas. Não apenas expondo contextos, mas casos de uso, ações de contorno, e sugestões de ação.	Fernanda Monteiro	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 17:40 <b>Room:</b> Ada Lovelace
<b>Xploit</b> Uma série especial que pretende municiar a sociedade civil com informações e soluções práticas para que Tecnopolítica deixe de ser um assunto aparentemente distante ou complicado.	TK	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 16:30 <b>Room:</b> Cinema Hacker

## HACKING

Título	Responsáveis	Data, Hora e Local
<b>CooLab MESH</b> Monte sua rede mesh em 15 minutos, usando o cozinheiro de firmware CHEF e o firmware libremesh!	bruno vianna	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 16:30 <b>Room:</b> Laje
<b>CR2017 CTF</b> Devido ao sucesso do CTF da CR2016, estamos elaborando uma nova competição, com desafios de segurança física como o lockpicking, explorar temas como a engenharia social e propor problemas de criptografia moderna e exploração de binários!	RTFM [ChOkO]	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 09:00 <b>Room:</b> Ian Murdock
<b>Experimentando Fuzzing com o ZAP</b> Esta apresentação pretende introduzir conceitos gerais sobre fuzzing, falar sobre o projeto open source ZAP e mostrar alguns exemplos reais de uso das técnicas para testes de penetração.	Maurício Harley	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 12:00 <b>Room:</b> Aaron Swartz
<b>Hackeando APPs</b> Aprenda como hackear o tráfego de informações dos APPs que você utiliza.	Tobias Sette	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 19:20 <b>Room:</b> Edward Snowden
<b>Inimigo íntimo</b> Será demonstrado como um atacante pode comprometer os endpoints, atacar a estrutura da rede e capturar informações de forma stealth entre outras técnicas.	Alex Nunes	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 02:00 <b>Room:</b> Aaron Swartz
<b>Pequenos e densos datacenters autônomos</b> Nesta fala encorajaremos a montagem de pequenos datacenters como hobby, diversão e atividade política importante para a diversificação e resiliência dos nossos sistemas computacionais.	hatto gus Alexandre Deckleva	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 15:20 <b>Room:</b> Laje
<b>Pwn3d IoT - Ataques massivos e Detecções</b> Será abordado o funcionamento de ataques em aplicações IoT's, desde o populamento de uma botnet utilizando dispositivos IoT's até o escopo final do ataque.	Jhonathan Davi	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 18:50 <b>Room:</b> Edward Snowden

Título	Responsáveis	Data, Hora e Local
		Snowden
<b>Revers@ndroid: recuperando seu Android de um ransomware</b> Vamos verificar como fazer a engenharia reversa de malwares da família Android/Lockerpin e obter a chave utilizadas para a encriptação dos arquivos.	Cassius Puodzius	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 16:30 <b>Room:</b> Aaron Swartz
<b>Sequestro 2.0</b> Serão mostradas as mais recentes técnicas de infecção; quais são os tipos de ransomware existentes; seu funcionamento; quais os impactos de uma infecção.	Raphael Jubram	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 18:50 <b>Room:</b> Aaron Swartz
<b>snifando celulares GSM com linux</b> O sistema telefônico de celulares GSms , sua constituição e a possibilidade de snifar o sistema com linux e radio SDR.	caio lucena	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 03:00 <b>Room:</b> Aaron Swartz

## KEYNOTE

Título	Responsáveis	Data, Hora e Local
<b>Keynote - Não começou com Snowden e não vai terminar com o Vault7</b> Palestra de abertura com James Bamford.	James Bamford	<b>Dia:</b> 05/05/2017 <b>Hora:</b> 20:30 <b>Room:</b> Chelsea Manning
<b>Keynote - Resistindo à distopia</b> As duas pessoas vão debater a necessidade de alertar acerca dos riscos de um futuro tenebroso, sem imobilizar grupos, coletivos e pessoas, mas, ao contrário, criando estratégias de resistência e mobilização.	Lili_Anaz Sasha	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 10:30 <b>Room:</b> Chelsea Manning

## CINEMA

Título	Responsáveis	Data, Hora e Local
Cinemhacker	lari	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 12:00 <b>Room:</b> Cinema Hacker

## RAVE

Título	Responsáveis	Data, Hora e Local
<b>4 0 4 0 4 0 4</b> A instalação conta com quatro vídeos, que ultilizam da estética do Glitch art para problematizar falhas estruturais do nosso sistema.	Jpedrinho9@	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 21:00 <b>Room:</b> Rave AlJaniah - Térreo
<b>Bora jogar ?</b> Uma sessão de uma hora para que os participantes da Cryptorave possam jogar um jogo de tabuleiro e receber dicas de segurança ao mesmo tempo.	ARTIGO 19	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 02:00 <b>Room:</b> Ian Murdock
<b>Cabeça em Movimento</b> Banda. Power trio com composições próprias influenciada pelo hard core, jazz e Baião.	Cabeça em Movimento	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 22:00 <b>Room:</b> Rave AlJaniah - Térreo
<b>DJ - CryptoRave</b> GSouts, atuante na área de T.I há 3 anos trabalhando com segurança da informação e Infraestrutura de computadores de dia. Já de noite sou Deejay de Deephouse music e Eletro trance nas ruas e cidades de SP.	GSouts	<b>Dia:</b> 07/05/2017 <b>Hora:</b> 00:50 <b>Room:</b> Rave AlJaniah - Mezanino
<b>Jogatina e Depravação com o Baralho OPSEC</b> Um ano após o lançamento do Baralho OPSEC, queremos proporcionar mais diversão este ano com uma nova edição do jogo, com mais cartas e mais possibilidades de comunhão com um mundo arredio em estado de crise.	rhatto gus	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 01:00 <b>Room:</b> Ian Murdock

Título	Responsáveis	Data, Hora e Local
<b>Poeticida</b> Experimental Music, Trance, Abstract Music, Eletronic, Synth performance.	Poeticida	<b>Dia:</b> 07/05/2017 <b>Hora:</b> 03:00 <b>Room:</b> Rave AlJaniah - Térreo
<b>Rapfunkcumbiapsicodeliafrobeatragga</b> Música regional encontra sintetizadores e remixagens, com ritmos diversos do Brasil e América Latina - com uma pitadinha de sul global e de sacanagem feminista.	Ocarina	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 22:00 <b>Room:</b> Rave Al Janiah - Mezanino
<b>Show Devilish</b> Paulo Ratkiewicz – guitarra e vocais Éder Chapolla – bateria Caíque Fermentão – baixo	Devilish	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 23:10 <b>Room:</b> Rave AlJaniah - Térreo
<b>Show do Retrigger</b>	Retrigger	<b>Dia:</b> 07/05/2017 <b>Hora:</b> 02:00 <b>Room:</b> Rave Al Janiah - Térreo
<b>Sideralismo</b> Sideralismo é uma proposta que leva a experiência cotidiana urbana e política ao espaço festivo, através de um live set sonoro e visual manipulado em tempo real.	tatianatr	<b>Dia:</b> 06/05/2017 <b>Hora:</b> 23:40 <b>Room:</b> Rave Al Janiah - Mezanino

A CryptoRave inspira-se na ação global e descentralizada da CryptoParty, a qual têm como objetivo difundir os conceitos fundamentais e softwares básicos de criptografia. Criada em 2014, a cada edição mais de 2500 pessoas participaram!

### **Programe-se!**

A CryptoRave 2017 será realizada na Casa do Povo, no dia 5 e 6 de maio de 2017, a partir das 18h do dia 05 (sexta-feira) até às 19h do dia 06 (sábado)

A Festa no Al Janiah começa na sequência, às 20h do dia 06 (sábado)



#### **Casa do Povo**

Rua Três Rios, 252 - Bom Retiro - São Paulo

#### **Al Janiah**

Rua Rui Barbosa, 269 - Bela Vista - São Paulo