16 de dezembro de 2014
Índios protestam em frente ao anexo 3 da Câmara dos Deputados, por causa da votação de proposta de emenda à Constituição (PEC) que trata da demarcação das terras indígenas.

ESCOLA DE ATIVISMO

[ABRIR EL CÓDIGO]

GUÍA DE FACILITACIÓN Y APRENDIZAJE DE SEGURIDAD DE LA INFORMACIÓN

GUÍA DE FACILITACIÓN Y APRENDIZAJE DE SEGURIDAD DE LA INFORMACIÓN

Este material es el resultado de una compilación de estudios, información y textos producidos por el Núcleo de Seguridad de la Información de la Escuela de Activismo, con el objetivo de subsidiar los procesos de aprendizaje desarrollados en los últimos años.

Más que comprender y usar correctamente las herramientas de Seguridad de la Información, es necesario desarrollar una cultura de seguridad que va más allá de su grupo u organización y se extiende también a su red de socios y aliados.

La jornada de aprendizaje sobre seguridad es un proceso constante y se muestra más eficiente cuando se comparte colectivamente. Durante este proceso, las habilidades de creación, facilitación y organización de procesos de aprendizaje son tan importantes como los conocimientos y técnicas de Seguridad de la Información.

Este material comenzó a reunirse en el 2017, con el objetivo de ser un punto de partida para una sistematización de conocimientos relacionados con la facilitación de procesos de aprendizaje sobre Seguridad de la Información. Sin embargo, algunos contenidos son temporales y pueden contener información o procedimientos obsoletos.

Esta guía se pensó para ser una colección libre y en constante transformación. Corrige los textos, contesta los argumentos. Estimule su mente y siga sus propias reflexiones.

Déjate llevar, anota, garabatea y cambia el orden, después de todo, el viaje ahora es tuyo.

¿Vamos juntos? Envía tus aportes, críticas y comentarios a suporte@ativismo.org.br

COLABORADORES

Amarela, Carla Jancz, Carolina Munis, Fernanda Shirakawa, Foz, Gabi Juns, Gustavo Gus, Lucas Malaspina, Luciana Ferreira, Marcelo Marquesini, Narrira Lemos, Mirim, Violeta Cunha.

Revisión: Bruno Freire.

COLABORA CON ESTA GUÍA

suporte@ativismo.org.br

CONTENIDO

[Introducción]

En esta sección, preparamos una introducción al aprendizaje de la Seguridad de la Información, que depende de varios factores que van del contexto socio-político a la utilización de las herramientas. Producimos este material para que lo utilicen grupos activistas que tengan interés en profundizar, descubrir y crear metodologías propias para la construcción de procesos de aprendizaje en esta área.

ÁGUILA - LA GUÍA

Mientras que el flujo de las comunicaciones de la sociedad se da cada vez más en el ambiente digital, la vigilancia y el monitoreo se han convertido en prácticas valiosas y bastante comunes en el campo de las disputas políticas y sociales.

¿Por qué Águila - La Guía?

Según el diccionario de símbolos, el águila es un animal solar y celeste, símbolo de la fuerza, vitalidad y protección. Muy ágil y habilidosa, esta ave también está relacionada con la realeza y los Dioses por la perspicacia de su mirada, pues le permite ver el Sol directamente. Un símbolo de clarividencia.

Se considera un animal psicopompo, del griego psychopompós, unión de las palabras psykhé, que significa "alma", y pompós, que significa "guía". El águila, así, tiene el sentido de orientar situaciones de iniciación o de transición.

En este sentido, nuestra guía pretende ser un Águila. Por servir de orientación, una referencia para que tus estudios y aprendizajes sobre el campo de la Seguridad de la Información no queden restringidos, sino que puedas llevarla y recurrir a ella cuando sea necesario.

En este material, encontrarás algunas posibilidades de lecturas como una base de sustentación para los movimientos del pensamiento y de la acción con organizaciones y grupos. Contiene, además, referencias para que construyas tu taller o actividad teniendo en cuenta aspectos básicos o más sofisticados, según el grupo y la necesidad.

Todo esto de un modo inventivo: este es el modo en que se basa la Escuela de Activismo para realizar sus procesos de aprendizaje, incentivando la multiplicación, la edición y la producción de conocimientos.

La Guía procura ser también una referencia para una forma de realizar procesos formativos que incentiva la inquietud, con prácticas de ampliación de la experiencia de las personas participantes con el pensamiento y con la acción. No solo es un cuaderno con recetas, sino que nos invita a formular buenas preguntas. Ofrece pistas para un camino que se hace al andar, más que trayectorias definidas.

Te deseamos una gran experiencia de lectura, estudios y aprendizaje.

Escuela de Activismo
16 de septiembre de 2017

APRENDIZAJE DE SEGURIDAD DE LA INFORMACIÓN

El contexto del aprendizaje de Seguridad de la Información.

En un universo tecnológico cada vez más dilatado, el aprendizaje de Seguridad de la Información (SI) representa un desafío. En nuestra opinión se produce solo si hay una necesidad, un deseo de aprender, ya sea para protegerse a uno mismo, a algo o alguien, para actualizarse a uno mismo, o para romper con ciertas estructuras de captación del pensamiento y los cuerpos.

Un segundo factor importante en este proceso es la comprensión de que vivimos en constante proceso de alfabetización, como diría el educador Álvaro Vieira Pinto, pues nunca seremos alfabetizados en todos los temas o asuntos. Siempre habrá algo nuevo que aprender y que enseñar.

Y un tercer factor considerable para el aprendizaje en SI son los métodos utilizados. Sabemos que, en nuestra vida cotidiana, existen diversos medios para facilitar la vida. Nuestra experimentación se reduce a algo que es práctico, rápido y de fácil absorción; por lo tanto, estamos cada vez más lejos de un proceso de aprendizaje complejo. En este sentido, es necesario obtener una comprensión política de estos sistemas y herramientas, para iniciar un proceso de distanciamiento de lo que se nos ofrece y una transición hacia otros sistemas. Se trata de evitar instrumentos de captura y vigilancia por medio del conocimiento de herramientas que procuran la independencia de las estructuras de poder, lo que exige dedicación y atención por parte del alumno.

Como consecuencia, es necesario que las herramientas de Seguridad de Información se presenten junto con el contexto vivido, para problematizar su utilización. El acompañamiento de este proceso también es fundamental; hay que tener a alguien que entienda del asunto a quien recurrir cuando surgen dudas u obstáculos.

El aprendizaje de la Seguridad de la Información puede llegar a ser significativo si hay intervención mutua entre los siguientes factores: las necesidades del aprendiz, la comprensión del contexto social, político, tecnológico y ambiental, y la facilitación de herramientas funcionales con el debido acompañamiento en su implementación.

15 de outubro de 2013
Ato III - Um milhão pela educação

[pretaller]

Antes de realizar un taller, recomendamos pensar y elaborar algunos puntos para su realización. Estos puntos pueden ser reflexiones acerca de las siguientes preguntas: ¿Cuándo necesitamos un taller de Seguridad de la Información? ¿Por dónde empezar? ¿Qué necesitamos para hacerlo posible? Además, ofrecemos una sugerencia para la creación de lineamientos, que podrá ayudarte a construir la metodología y visualizar el progreso de las actividades.

CUÁNDO HACER UN TALLER

El aprendizaje de la Seguridad de la Información se puede implementar de diferentes maneras. Una posibilidad es utilizar el modelo de taller, que permite un intercambio de experiencias y realidades entre las personas participantes y que, si se conduce bien, puede crear un ambiente en el que todos aprendan con todos y permitir que emerjan buenas posibilidades de uso de la SI por parte el grupo. Pero, ¿cuándo y cómo se debe realizar un taller?

El aprendizaje de la Seguridad de la Información para adultos implica cambio de hábitos, de creencias consolidadas e incluso de cultura en relación con la tecnología. Implica comprender lo que representa o no un riesgo y una amenaza para ti, tu grupo y tus actividades.

El modelo de taller prevé una interacción mayor entre las personas facilitadoras y las personas participantes en el proceso de aprendizaje, y se debe pensar desde esta perspectiva. Pero el aprendizaje comienza con el interés de la persona o grupo aprendiz. Y ese interés puede venir de varios factores: necesidad, curiosidad o deseo de saber más sobre el tema en cuestión.

El grado de interés del grupo a ser beneficiado afectará directamente a la decisión de optar o no por hacer un taller en un momento dado. Por lo tanto, antes de tomar la decisión de realizar un taller, verifica el grado de interés de tu grupo o de las personas que participarán en el proceso en relación con el tema que se va a abordar.

Comprueba, además, cuáles son las necesidades específicas de aprendizaje que tienen. Esto se puede hacer a través de cuestionarios, entrevistas, seguimiento de las personas en su día a día, investigación directa o (menos eficiente) información secundaria proporcionada por alguien o adquirida en informes y otras fuentes. Estos mecanismos ya pueden ser un primer canal de participación de las personas.

El interés y la necesidad influencian el diseño de tu taller y la elección de las personas facilitadoras. Puede determinar, por ejemplo, si necesitas trabajar más con información general y de contexto para generar sensibilización e implicación con el tema en cuestión. O, en el otro extremo, puede establecer si ya es el momento de dar prioridad a las actividades centradas en las soluciones y los cambios deseados, tales como la instalación y el uso de nuevas aplicaciones *(apps)* y programas *(software)* y los cambios en las rutinas y hábitos.

Recuerda que el tema abordado y el método utilizado se deben pensar y definir minuciosamente. Un taller no debe ser una secuencia de conferencias encadenadas a partir de una cierta lógica. ¡Puede incluir interacción, espacios para compartir y ser inclusivo! Cada persona adulta tiene su manera única de aprender. Las personas con mayor dificultad de aprendizaje pueden llegar a ser las más vulnerables.

Facilita la participación a través de debates, juegos, actividades recreativas y otras herramientas. Cuanto más involucradas y activas se sientan las personas en el proceso, mayor será la probabilidad de que el taller alcance sus objetivos.

Si detectas que el interés de los potenciales participantes no es suficiente para la realización de un taller, se pueden explorar otras alternativas iniciales: promover ruedas de diálogos sobre el tema, distribuir textos, videos, invitar a las personas a dar conferencias, etc. En resumen, ¡crear un clima!

Por último, ten en cuenta que el aprendizaje de Seguridad de la Información depende, por encima de todo, de cambios de comportamiento, cultura y hábitos a nivel individual y, principalmente, de grupo. Un taller, por sí solo, no es suficiente para engendrar esas transformaciones. Por lo tanto, considera el aprendizaje como un proceso a medio y largo plazo. Comienza poco a poco, planifica un objetivo simple para tu taller y colócalo dentro de una estrategia más amplia de aprendizaje.

PLANIFICACIÓN DE UN TALLER

Cómo planificar un proceso de aprendizaje: las 3 fases y los momentos esenciales de un taller.

Una forma eficaz de estructurar la planificación de un taller de Seguridad de la Información es dividir el proceso en 3 etapas: PRETALLER, DURANTE EL TALLER y POSTALLER

Cada proceso de aprendizaje tendrá sus necesidades y características propias, pero algunas actividades son comunes en varios tipos de taller. Vamos a resumir cada una de estas etapas e incluiremos algunas preguntas que te ayudarán a pensar y organizar este proceso.

PRETALLER:
La etapa "pretaller" va desde el momento en que el taller es concebido como propuesta hasta la recepción de las personas participantes. Normalmente, implica hacer una buena evaluación de las necesidades del grupo, planificar el itinerario, determinar las necesidades de espacio y de materiales y comunicarse con los participantes de manera mínimamente segura.

¿Cuáles son las principales necesidades del grupo? Comprueba las demandas que tiene el grupo en su vida cotidiana y en su trabajo y que transforma en necesidades de aprendizaje.

¿Qué hábitos y prácticas poseen actualmente las personas participantes? Busca el perfil, la infraestructura digital utilizada y los hábitos digitales de las personas participantes. Es fundamental conocer los sistemas operativos utilizados, para cerciorarse de que las personas facilitadoras dominan su funcionamiento y el de las herramientas que se adaptan a ellos.

¿Cuál es el grupo de personas facilitadoras necesarias para realizar el taller? Piensa en los perfiles necesarios y en el número de personas suficiente para un seguimiento adecuado del grupo.

¿Qué habilidades y conocimientos queremos desarrollar hasta el final del proceso? Establece objetivos de aprendizaje basados en las necesidades del grupo y en lo que tú y tu equipo pueden ofrecer. Pero recuerda: en el momento de realizar el taller, aparecerán factores inesperados o no detectados anteriormente. Por eso, mantén la mente abierta para cambiar la dimensión de dichos objetivos durante el taller y transforma las sorpresas en riquezas. ¡El proceso está vivo!

¿Qué reflexiones y encadenamiento de ideas queremos provocar en cada sesión? Diseña lineamientos que conduzcan a los objetivos de aprendizaje de forma fluida y satisfactoria. Y, nuevamente, es importante estar preparado para cambiar el recorrido si la necesidad del grupo cambia durante el taller. Ver más en la sección "Lineamientos".

¿Qué materiales serán necesarios para desarrollar cada actividad? Una sugerencia es elaborar un itinerario de taller que contenga las dinámicas propuestas y los materiales que cada una de ellas utilizará.

¿Cuántos recursos financieros serán necesarios para la realización del taller? Considera la remuneración o la retribución para las personas facilitadoras, alimentación, transporte y otros factores.

¿Qué procedimientos logísticos son necesarios para realizar el taller? Ver más en la sección "Preparación de un taller: logística operacional".

DURANTE EL TALLER:
la etapa "durante el taller" va desde la recepción de los participantes hasta la sesión de cierre, e incluye tanto las actividades de aprendizaje como los momentos entre las sesiones. Toda interacción entre el grupo y entre las personas facilitadoras es una oportunidad de aprendizaje. Por eso también es importante entablar un diálogo en el grupo de facilitación que está conduciendo el proceso a fin de evaluar el progreso de las actividades y perfeccionarlas para satisfacer las necesidades del grupo.

¿Cómo es el nivel de energía y de atención del grupo? Las pausas son tan importantes como las sesiones. En este momento el equipo facilitador puede detectar cómo está el grupo, quién está logrando acompañar y quién tiene dificultad. Busca detectar la necesidad de dar un intervalo o de cambiar la energía de la sala.

¿Cómo mantener el clima y la atención en las actividades? Saber identificar qué tipo de "clima" requiere cada sesión y poder mantenerlo es una parte fundamental del aprendizaje. Algunas sesiones requieren un ambiente más silencioso, meditativo y propicio para la concentración profunda. Otras precisan más dinamismo, participación y movimiento. ¡Piensa en maneras creativas de lograrlo!

¿Cómo seguir activando e involucrando al grupo? En tu taller, evita intentar involucrar o sensibilizar a las personas participantes a través del "susto", es decir, utilizando el miedo del monitoreo, de la vigilancia o de la citación de casos reales de falla de la seguridad. Hay un riesgo alto de que muchas personas opten por la alienación, el descrédito o la contestación pura y simple, sin abrirse al aprendizaje.

¿Cómo vamos a monitorear si las personas participantes están aprendiendo? Al construir formas de evaluación y seguimiento del aprendizaje mientras se realiza el taller.

¿En qué condición está el equipo de facilitación? El equipo necesita verificar constantemente cómo están las personas integrantes: si hay sentimientos de sobrecarga, ansiedad, frustración, o incluso confianza excesiva. Esta forma de autocuidarse y cuidarse de sí es esencial para un buen ambiente de aprendizaje y para que las personas facilitadoras puedan conectarse a las necesidades del grupo.

¿Los objetivos de aprendizaje diseñados inicialmente todavía tienen sentido? Reúna al equipo en momentos clave durante el taller para evaluar si los objetivos, diseñados a partir de las necesidades identificadas en la etapa pretaller, todavía se corresponden con la realidad del grupo durante el taller.

¿El lineamiento original aún tiene sentido? Comprueba que las sesiones propuestas de hecho conduzcan a los objetivos, principalmente si se han rediseñado.

POSTALLER:

El desarrollo de conocimientos y habilidades no se termina al final de un taller. Es importante establecer algún tipo de apoyo y seguimiento de la evolución del grupo. La creación de canales de comunicación o la producción de materiales de apoyo y otras formas de apoyo al aprendizaje son esenciales para ayudar en la jornada de adquisición de conocimiento.

¿El grupo necesitará un seguimiento posterior al taller? La necesidad de acompañamiento puede surgir de varios factores, como el uso de herramientas recién incorporadas, el apoyo en la multiplicación de los conocimientos para los grupos y organizaciones de las personas participantes, o ayuda para personas que no hayan consolidado el conocimiento en uno o más temas del taller.

¿Qué recursos y sistemas necesitamos crear para llevar a cabo este seguimiento? Planifica los canales de comunicación, plataformas, materiales, tiempo y recursos financieros necesarios para realizar el seguimiento.

PREPARACIÓN DE UN TALLER: LOGÍSTICA OPERACIONAL

Para preparar un taller es necesario, antes que nada, entender cuál es la demanda del grupo, del lugar y del tiempo necesario. Las listas de verificación, o checklists, son grandes aliadas para garantizar que no se deje nada de lado. La comunicación con las personas involucradas también es una práctica fundamental, sea con el grupo de participantes o de facilitadores. Y en caso de duda, ¡siempre pregunta!

Es fundamental que la persona o el equipo responsable de la logística esté en contacto constante con las personas facilitadoras del taller. De esta podrán entender cuál es el objetivo del encuentro, su duración prevista, las demandas de estructura necesaria, el tamaño del grupo y el perfil de las personas participantes.

El mejor recurso para el seguimiento de las necesidades de logística es la lista de verificación, o *checklist,* que ayuda a garantizar que no se deje nada de lado.

¿Cuál es el objetivo del taller? El objetivo puede influir en el lugar elegido, la forma en que se establece la comunicación con las personas participantes, y los recursos necesarios.

¿Cuál es el presupuesto disponible para el taller? Comprueba el presupuesto total y el presupuesto para cada elemento, como la alimentación, el transporte, el lugar y el seguro (si hubiera). Controla la ejecución de cada gasto y, si es necesario, negocia con el equipo facilitador la transferencia de recurso de un elemento a otro.

¿Cuál es el tamaño y el perfil del grupo? Pregunta la edad, necesidades especiales, dieta vegana o vegetariana, restricciones alimenticias, alergias, enfermedades crónicas, contacto de emergencia y otros factores. Otro punto a destacar es que las necesidades de comunicación y relación con el grupo cambian si las personas participantes son de la misma organización que tú, de otra organización única o de diferentes organizaciones y localidades.

¿Cómo será la alimentación durante el taller? Si el taller provee alimentación, asegúrate de que haya vajilla y cocina de apoyo en el lugar elegido. Y, sobre todo, prepara un menú que encaje en el presupuesto y que sea acorde a las necesidades de las personas participantes. Por último, ¡no olvides planificar el suministro de agua potable y el infaltable café!

¿Cuál es el lugar ideal para el taller? La ubicación debe cumplir con todos los factores enumerados anteriormente. Y, además, asegúrate de que satisfaga las necesidades básicas: mesas, sillas, tomacorrientes, pizarra negra/blanca, rotafolio, proyector, reproductor de sonido, pared para proyección, pared para pegar tarjetas o carteles, y espacio para trabajos en grupo y en plenaria.

Es importante verificar también el estado de los baños, la ventilación, la iluminación y las interferencias externas, como el ruido de la calle. Además, procura asegurar que el día del encuentro todo esté limpio y en orden.

Realiza al menos una visita técnica al lugar, preferentemente el mismo día de la semana y en el mismo horario en que se llevará a cabo el taller para saber qué esperar.

¿El grupo necesitará un seguro de vida o equipo? Prevenir incidentes puede traer más tranquilidad y reducir el costo. Si el seguro es una posibilidad, verifica si hay presupuesto disponible para ello y reúne la información necesaria (ver más sobre cómo recolectar dicha información en la sección "Comunicarse de forma segura con las personas participantes").

¿Cuáles son los materiales necesarios? Pide al equipo facilitador que enumere todos los elementos necesarios y los proporcione. Por ejemplo: Internet, papel sulfito, bolígrafos, marcadores, tiza para pizarra, cinta adhesiva, credenciales, extensiones, materiales impresos, etc.

COMUNICACIÓN SEGURA CON LAS PERSONAS PARTICIPANTES

Es común que las personas que participan en procesos de aprendizaje de Seguridad de la Información se preocupen por la seguridad de sus comunicaciones o estén en situación de amenaza o monitoreo. Por ello, es importante ofrecer herramientas seguras para la comunicación que precede al taller, cerciorándose de que las personas participantes quieran y sepan utilizarlas.

Planifica y prepárate para hacer contacto constante con las personas que participan en el taller. Es común que tengan varias preguntas, peticiones y comentarios en el período anterior al proceso. Si es posible, asigna a una persona que se dedique exclusivamente a esto.

Intenta entender el contexto en el que se encuentran las personas participantes, el grado de seguridad necesario para cada una de ellas y si se encuentran cómodas al usar herramientas de comunicación más seguras. Si las condiciones y las necesidades conllevan utilizar herramientas más seguras, explícalo de forma clara y resumida. Evitar canales de comunicación como *Whatsapp, Facebook* o *Gmail* e indíqueles a las personas que utilicen herramientas como *Jitsi* (para conversaciones de audio y vídeo en línea), *Signal* (para hablar por teléfono o computadora) o correos electrónicos cifrados (ayudar a crear una cuenta de correo electrónico de *Riseup).* Sin embargo, asegúrate siempre de que el uso de estos recursos sea viable para la persona participante y que no impedirá su comunicación, especialmente en la importante etapa de pretaller.

Al pasar a reunir datos e información de diferentes personas, principalmente de activistas, es muy importante que cuentes con un protocolo de seguridad. Tanto tu lista de posibles participantes o de invitados como la lista de participantes confirmados del taller deben estar guardadas de manera segura. A menos que estés usando un servidor de confianza para el almacenamiento en línea, elije la carpeta encriptada en tu equipo y accede preferentemente sin conexión. Evita relacionar el nombre de las personas al área de actuación o región en que vive, y aprovecha para liberar la imaginación y crear apodos para identificar a los participantes de las listas.

El lugar y la fecha de realización del taller también son información muy sensible y requieren cuidado. Intenta divulgar esto a los participantes lo más cerca posible de la fecha de la realización: así se evita que el lugar reciba atención o haya intentos de interferencia. Un consejo es avisar con antelación la región en que se realizará el taller sin indicar la dirección exacta, y comunicar esta información sólo cuando los participantes estén a punto de salir de casa, en caso de transporte individual, o ya en el camino del encuentro, en caso de transporte grupal. Al hacerlo, organiza la información más importante en un boletín que debe incluir como mínimo lo siguiente: *fecha y hora, lugar, cómo llegar, lo que la persona participante necesita llevar.*

LINEAMIENTOS

Elaborar lineamientos te ayudará a planificar el tiempo de la actividad o taller y recordar lo que tienes que hacer. Es como un itinerario tradicional, pero incluye el tiempo, el objetivo, los materiales que necesitas y el contenido que vas a cubrir.

Al ser una persona facilitadora de Seguridad de la Información, a menudo serás quien va a introducir por primera vez a alguien en el mundo de la seguridad digital; lo que digas tendrá un gran impacto en cómo la gente piensa acerca de este tema. ¡Un pésimo primer entrenamiento de seguridad puede ser tan malo como o peor que ningún tipo de entrenamiento! Sin una estructura, podemos perder fácilmente los objetivos de la actividad y perjudicar a nuestro público, más que conquistarlo. Por eso, es necesario un entrenamiento bien estructurado, con el tiempo, los objetivos y los resultados que se desea alcanzar.

Es importante que la estructura de tu entrenamiento tenga en cuenta el objetivo de cada actividad y, consecuentemente, varíe en relación con él. Además, el tiempo, el espacio y los materiales disponibles para realizar la actividad también interfieren en el proceso en sí. Según el tamaño y el tiempo del taller (unas horas, uno, tres o hasta diez días), puedes crear lineamientos resumidos o un itinerario detallado. El itinerario resumido se puede entregar a las personas participantes del taller, mientras que el detallado lo podrás utilizar tú a lo largo de la actividad.

Generalmente, dividimos nuestro itinerario de actividades o taller con base en las sesiones; entonces, si planificaste un día de varios talleres/sesiones, podrías diseñar un lineamiento para cada uno de ellos. Tenemos un ejemplo que se puede utilizar como base para que construyas lineamientos para tu grupo, pero recuerda adaptarlo de la mejor manera para ti y tu grupo.

SUGERENCIA DE LINEAMIENTOS

[pretaller]

SESION: Coloca aquí el nombre de tu sesión. Por ejemplo: Introducción a la SI o Cifrado de correos electrónicos.

Nº. DE PARTICIPANTES: Es importante saber cuántas personas van a participar en tu taller, para saber, también, cuántas personas serán necesarias en la facilitación. Si es un taller de instalación, por ejemplo, sugerimos 1 persona facilitadora por cada 5 participantes.

OBJETIVO: Describir el objetivo de esta sesión. Esto te ayudará a pensar cómo organizarla y, también evaluar, al final, si lograste alcanzar tu propuesta. Iniciamos los objetivos siempre con verbos: Alcanzar, proporcionar, experimentar, mostrar, crear, registrar y otros que muestren la intencionalidad de una acción.

CONTENIDO: Los contenidos se refieren a los temas trabajados. ¿El contenido del taller es de introducción, básico, intermedio, avanzado? ¿Cuál es el tema principal? ¿Cuáles son los temas secundarios?

METODOLOGÍA/COMO PROCEDER: La palabra *metodología* deriva de "método", del latín "methodus" que *significa* "camino o ruta para lograr algo". Esta parte es muy importante. Es donde describimos, paso a paso, cómo se realizará la actividad, inclusive el tiempo que se invertirá en cada punto. Estate atento a esta descripción para que te ayude al momento de realizar la actividad. La medición del tiempo es importante, pero no puede representar una restricción. Siempre es posible revisar o cambiar el tiempo de acuerdo con el progreso del aprendizaje y del grupo. El objetivo de los lineamientos es ayudarte durante el taller, y no al revés.

Ejemplo de descripción del método y tiempo:

Sesión 1:

> Explicar cómo funcionará la actividad. Dividir en grupos a las personas que participan. 5'
> Iniciar la conversación según la primera ronda de preguntas. 20'
> Incorporar la segunda ronda de preguntas como estímulo para la continuidad de la conversación. 10'
> Iniciar la tercera ronda de preguntas como estímulo final para la conversación. 10'
> Solicitarle a cada grupo que resuma su comprensión sobre el tema. 5'
> Para finalizar, cada grupo comparte su resumen. 3' por grupo
> Espacio final libre para comentarios con palabras individuales. 2' por persona.

REFERENCIAS: Las referencias pueden ayudarte a construir el contenido y, además, pueden ayudar a la próxima persona que va a llevar a cabo dicha sesión.

TIEMPO: Coloca aquí el tiempo total de la sesión.

MATERIALES: Enumera los materiales que se van a utilizar (cantidad de mesas, sillas, cartulinas, bolígrafos, post-it, entre otros).

CONSEJOS: Hacer una buena selección de preguntas como estímulo e inducción de conversaciones. Contar con preguntas adicionales/alternativas para dinamizar las conversaciones de acuerdo con el perfil de las personas participantes. Adaptar el tiempo de duración de la sesión según el número de participantes. Imprimir la cantidad de preguntas según el número de grupos.

ETIQUETAS: ¿Cuáles son las principales categorías de esta sesión? Enuméralas aquí (por ejemplo, seguridad, criptografía, correo electrónico, etc.).

HORA EN LA PRÁCTICA
EJEMPLO DE LINEAMIENTOS A CUMPLIR

SESIÓN:

Nº. DE PARTICIPANTES:

OBJETIVO:

CONTENIDO:

METODOLOGÍA/COMO PROCEDER:

REFERENCIAS:

TIEMPO:

MATERIALES:

CONSEJOS:

ETIQUETAS:

[durante el taller]

Un taller de Seguridad de la Información es un encuentro de personas que intentan aprender más y juntas. Durante el taller, los facilitadores y participantes buscan interactuar en simbiosis. En esta sección, damos algunos consejos para que esto suceda en armonía en ambos grupos, la alineación de expectativas y la construcción de acuerdos

Israel Campos | @Bloco Sagrada Profana 2017

MOMENTO INICIAL

El Momento Inicial es esencial para ganar la confianza del grupo y establecer un ambiente con buenos vínculos para el aprendizaje.

La apertura, o el momento inicial del taller, es fundamental para establecer las expectativas y crear un ambiente acogedor de aprendizaje entre las personas participantes. Crear las bases de confianza entre ellas y el equipo de facilitación es esencial para el buen desarrollo del taller. Durante el Momento de Apertura, se deben considerar los siguientes pasos:

- Presentaciones del equipo que organiza y facilita la actividad o taller.
- Presentación de las personas participantes.
- Expectativa de las personas participantes.
- Programa o lineamientos del encuentro.
- Información logística y otra información pertinente.

Charla inicial del equipo sobre la actividad

La charla inicial del equipo es importante para darle la bienvenida a las personas presentes y ayudar a crear un buen ambiente para el inicio de las actividades.

Presentación del equipo o la persona facilitadora

La presentación del equipo o la persona facilitadora sirve para compartir con el grupo los papeles y funciones de cada persona durante el taller. La persona facilitadora puede incluir un breve resumen de su experiencia en el tema, de ser necesario.

Presentación de las personas participantes

En el campo de la Seguridad de la Información, es posible que las personas participantes se resistan más a compartir información personal al principio del taller. Una idea es comenzar con actividades de reconocimiento de grupo, como agrupar personas por hábitos similares. Otra sugerencia es iniciar las presentaciones en grupos menores antes de que las personas participantes se presenten ante todo el grupo. En el caso de grupos de conocidos, esta sesión se puede adaptar, como por ejemplo al compartir un asunto en pares que luego se comparte.

Alineación de expectativas

Toda persona participante llega al evento con una serie de expectativas y necesidades, que pueden o no coincidir con los objetivos generales del taller. Es importante hablar sobre las expectativas y, dentro de lo posible, incorporarlas al taller. Los acuerdos comunes, cuando son visibles para todo el grupo, generan responsabilidad compartida sobre los objetivos de la actividad.

Lectura colectiva del programa o lineamientos del encuentro

Hacer una lectura colectiva de la agenda del día, destacando los temas principales, los objetivos de cada sesión y los resultados esperados, ayuda a minimizar la desconfianza e inseguridad de las personas participantes al principio del taller.

Información logística y acuerdos de convivencia y seguridad
Reserva un momento para aclarar y acordar las principales cuestiones logísticas y operativas del taller:

> Presentación general del lugar
> Alojamiento, si se quedan durante la noche
> Horario de inicio, cierre e intervalos
> Alimentación
> Transporte de vuelta
> Pactos de seguridad (ver más en la sección "Comunicarse de manera segura con las personas participantes")

ACUERDOS DE CONVIVENCIA Y ESPACIO SEGURO

[durante el taller]

Garantizar un espacio seguro para el intercambio de experiencias y de conocimientos es importante para el bienestar del grupo y fundamental para el aprendizaje.

En el contexto del aprendizaje adulto y principalmente en el tema de la Seguridad de la Información, la relación establecida entre el equipo de facilitadores y las personas participantes debe ser más una asociación que una relación jerárquica. La construcción de confianza y respeto mutuo entre el grupo es esencial para el buen desarrollo del taller, ya que los talleres de SI normalmente tratan información sensible que puede poner en riesgo no sólo a las personas participantes, sino a todos los individuos implicados.

Con el fin de garantizar un espacio seguro para el intercambio de información y aprendizaje, el grupo puede establecer un acuerdo sobre reglas mínimas de convivencia. Tales acuerdos son establecidos por las propias personas participantes y se debaten con el grupo hasta que alcanzar un consenso o consentimiento. Los acuerdos deben permanecer visibles para las personas participantes durante todo el taller y cualquier persona puede llamar la atención del grupo con respecto a una de las reglas si siente que ha sido violada. Los siguientes temas pueden servir como punto de partida para establecer este acuerdo, pero es importante que se exploren otros temas relacionados con el contexto específico de tu taller.

Cumplimiento de horarios y puntualidad: Acuerdos sobre el horario de inicio, cierre y duración de las sesiones, incluidos los intervalos, las comidas, etc.

Presencia y participación: Las personas participantes deben comprometerse a estar presentes física y mentalmente en todas las sesiones, con atención especial para la navegación de Internet, verificación de correos electrónicos y utilización de redes sociales.

Ordenadores y teléfonos: Cuando sea necesario, debe existir un acuerdo sobre el uso de ordenadores y teléfonos durante las sesiones, y sobre qué hacer cuando el uso de estos aparatos no esté permitido.

Fotos y redes sociales: Los Talleres de Seguridad de la Información normalmente son eventos reservados, pero los participantes no siempre conocen esta costumbre, por lo que es importante pactar cuestiones como la toma de fotos o las publicaciones en las redes sociales sobre el evento. Si se permiten las publicaciones, es importante establecer reglas sobre las etiquetas y la ubicación. Y, si se permite tomar fotos, se debe especificar de quién, cuándo y dónde.

Seguridad física: La seguridad física de las personas involucradas en un taller debe ser una responsabilidad compartida entre todo el grupo. Por lo tanto, es importante establecer un pacto de no practicar ningún acto que ponga en riesgo la seguridad de alguna otra persona participante, organizadora o facilitadora, así como establecer un acuerdo máximo de no prender fuego el taller.

Política de descargas: Establecer un pacto de buen uso del Internet disponible es esencial para el éxito de un Taller de Seguridad de la Información. Esto significa asegurar que los programas que puedan afectar la conexión de los

demás participantes estén apagados, como Torrents, sincronizaciones de Dropbox, Google Drive y cualquier otro servicio que pueda generar tráfico en segundo plano, así como alertas y notificaciones que puedan interrumpir el buen desarrollo de las actividades.

Responsabilidad sobre el propio aprendizaje: La responsabilidad del propio aprendizaje es un acuerdo indispensable. Una buena conversación sobre las necesidades individuales y los acuerdos colectivos es siempre una buena opción en inmersiones, talleres y actividades.

Respeto en cuestiones de raza, etnia, género, identidad de género, orientación sexual, regionalidad y capacidad: La diversidad es, ante todo, una riqueza y un activo en cualquier ambiente de aprendizaje. Para tratarla como tal, es importante comenzar conversando colectivamente sobre el respeto y la valorización de la singularidad de cada persona y los términos y posturas que no se deben mencionar.

CIERRE - MOMENTO FINAL
EVALUACIÓN DE APRENDIZAJE

El término “evaluar” deriva del latín: VALERE, "ser fuerte, estar bien, tener valor". Es decir, la evaluación nos remite a atribuir valor a algo o a alguien. Incluso sin un ambiente definido, estamos en constante evaluación, evaluamos nuestro día, nuestras actividades, lo que vamos a comer, lo que vamos a vestir. La evaluación puede considerarse parte del aprendizaje. Por lo tanto, los espacios de evaluación sirven para determinar los elementos que agregaron valor a una persona o grupo, y se utilizan bastante para replantear acciones, actividades y procedimientos.

Evaluación de los participantes:
el momento de evaluación de una actividad o taller es una etapa del proceso de aprendizaje tanto para los participantes como para el equipo que ofrece la actividad.

Ofrece posibilidades para problematizar el espacio, los métodos, el contenido, la facilitación o la mediación de un proceso, los materiales disponibles, los alimentos y muchos otros elementos que quieras conocer, medir o asignar valor con el grupo.

En la residencia de la SI, el proceso de evaluación se produce a partir de una metodología denominada *de contorno*. En esta metodología, las personas participantes realizan el contorno de sus cuerpos, y a medida que las actividades van avanzando, realizan representaciones en el contorno con la ayuda de recortes, dibujos y símbolos dibujados en la hoja. Los *Contornos* están expuestos durante toda la estadía, y a través de él, los participantes y el personal acompañan a los procesos de aprendizaje de cada persona y el grupo en su conjunto.

Este tipo de actividad confiere un modo diferente de realizar procesos de evaluación, ya que mide el aprendizaje más allá del lenguaje tradicional hablado. Busca escapar de los modos convencionales de transmitir información sobre una determinada situación y no impide compartir el afecto y el aprendizaje. Por el contrario, es válida la utilización de la imagen para entablar una buena conversación.

En los talleres o actividades cortas, llevar a cabo el *contorno* puede ser difícil para cumplir con el tiempo. Entonces, se puede realizar una evaluación con palabras libres, en una palabra, o al poner a disposición un folleto con preguntas y pedir que los participantes respondan y entreguen al final. En fin, existen varias posibilidades de evaluación, recordando que es esencial la adaptación conforme al grupo y el formato de la actividad.

Evaluación de equipo:
la evaluación realizada por el equipo se realiza cotidianamente, generalmente al final de los talleres o de las actividades del día. Sirve como guía para las próximas actividades. Expresan cómo se sienten las personas que están mediando la actividad, cuál es el clima del grupo e indica desafíos y posibilidades para las actividades. Es importante que en este momento las personas estén atentas a sus propios procesos de aprendizaje, pero principalmente al proceso de los participantes; en este punto, se deben evitar los desentendimientos y mantener un clima de complicidad en el equipo para

que el proceso, cuando sea extenso, se lleve a cabo de la mejor manera posible hasta su conclusión.

En ese sentido, el cuidado con el proceso es fundamental, y el itinerario de actividades representa un gran apoyo en este proceso de revisión o adaptación de lo que se logró y lo que se está haciendo. Con base en él podemos implementar las modificaciones que el equipo considere necesarias sin perder la Guía sustentadora del proceso.

Generalmente, en un proceso de evaluación, decimos qué cosas que marcaron nuestra presencia en las actividades. Elementos que pasan por la estructura física, por los contenidos, por las metodologías, pero también por aquello que más nos afectó. Lo que quedó de la actividad. Por eso, si el proceso de evaluación se realiza adecuadamente y hay un buen ambiente, proporcionará un buen aprendizaje y una buena replanificación de acciones.

Muchas veces esta evaluación no ocurre al finalizar un taller. Entonces, resulta necesario un tiempo de "decantación", un tiempo de lograr que "caiga la ficha" de los contenidos aprendidos. En este caso, utilizamos cuestionarios postaller, con preguntas muy abiertas. ¡También puedes utilizar el mismo seguimiento diario para evaluar o medir el aprendizaje!

Arthur Monteiro | @Congresso Nacional 2013

[postaller]

Dudas, sugerencias y cómo mantenerse en contacto son elementos que suelen surgir después de un taller o proceso de aprendizaje de Seguridad de la Información. Establece un canal con las personas participantes para que el aprendizaje continúe, ¡incluso después del taller!

SOPORTE TÉCNICO

El proceso de aprendizaje continuo por mucho tiempo después del taller, entrenamiento, charla, etc. Después del evento, existe una gran oportunidad para mantener a las personas interesadas en actualizarse y continuar aprendiendo, ya sea por medio de materiales u otro tipo de contacto. En la Seguridad de la Información, este proceso puede fortalecerse de forma digital.

Nuestro aprendizaje ocurre principalmente cuando tenemos ejemplos sobre el contenido, el intercambio de experiencias, o las personas asociadas y facilitadoras que nos acompañan. Por lo tanto, una forma efectiva de mantener el grupo en contacto es establecer un canal para ello: crear una lista de correos electrónicos (ver el tema *correo electrónico seguro* en Recursos). La lista de correos electrónicos puede servir para varios propósitos: solicitudes de ayuda, intercambio de información, debates generales y relatos de historias. Con esta lista, las personas facilitadoras tienen un potencial muy grande como fomentadoras de información y de debates, y además, pueden promover la interlocución y alentar los encuentros en línea y fuera de línea (por ejemplo, si el grupo reside en la misma ciudad).

Como soporte técnico, la persona que facilitó el encuentro debe estar siempre atenta a los canales de comunicación que se establecieron, para que quien pida ayuda u otro tipo de información no se quede con dudas, aunque sería interesante que otros participantes del grupo también respondan a las preguntas. Recuerda: tu opinión es muy importante para aquellos que recibieron tu entrenamiento.

Otras formas efectivas de mantener viva la producción de aprendizaje son a través de grupos de mensajería instantánea. Recomendamos la creación de tales grupos en los chats cifrados, como *Signal.* Si tu grupo de entrenadores es fijo y organizado, es posible crear otros canales de discusión, como boletines informativos, videos de entrenamientos e historias sobre el tema, páginas de Internet, entre otras opciones. De una manera u otra, es muy importante que haya una periodicidad mínima en la información que circula en el grupo: envía noticias y actualizaciones en el área de Seguridad, pregunta cómo están, si aprendieron algo nuevo, si tienen dudas, etc.

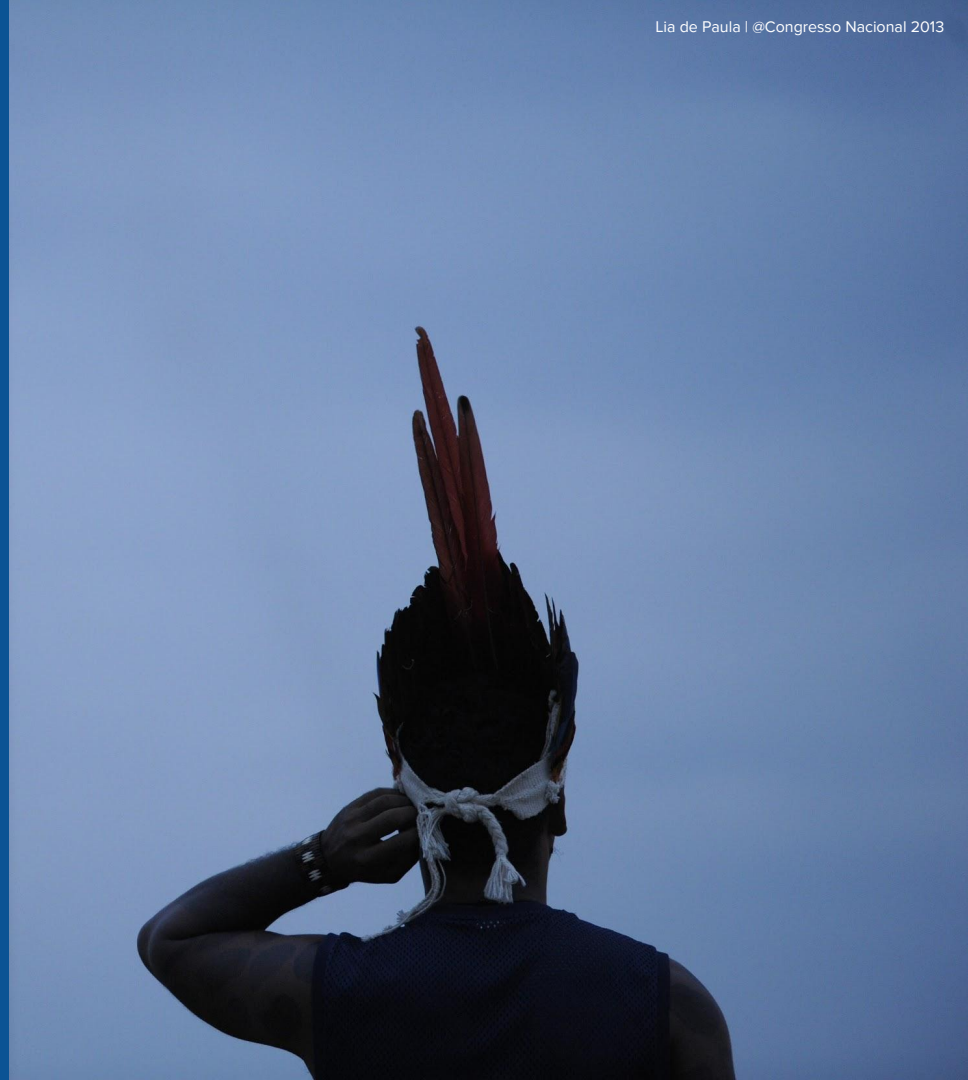
SUGERENCIA

Después del evento es muy común que las personas participantes se acerquen a ti para preguntar dónde buscar información o a quién recurrir cuando tengan dudas o quieran replicar el aprendizaje obtenido. Planifica estas respuestas y, si es posible, actúa con antelación: en la sesión final de tu entrenamiento, pregunta cuál es el mejor canal de comunicación para un posible soporte o para mantener el grupo en contacto: ¿una lista de correos electrónicos, un grupo de mensajería instantánea, o solo el correo electrónico de las personas entrenadoras disponibles?

Nuestra sugerencia es crear una lista de correos electrónicos: así, puedes mantener tu grupo unido, obtener un historial de las conversaciones en el soporte y determinar si va en el camino correcto para el aprendizaje y el entrenamiento grupal. ▪

[contenido de apoyo]

En esta sección, invitamos a las personas que actúan en el área de Seguridad de la Información en Brasil a ofrecer ayuda en la construcción del contexto de la vigilancia y de las herramientas utilizadas en Brasil. Debe servir de base para realizar conexiones con las herramientas en el momento de tu taller. Recuerda que esta área de conocimiento (al igual que todas las demás) está en constante cambio, y puede que algunos elementos ya se hayan transformado cuando accedas a este contenido, por lo que debes mantener tu aprendizaje siempre actualizado.



Lia de Paula | @Congresso Nacional 2013

INTRODUCCIÓN

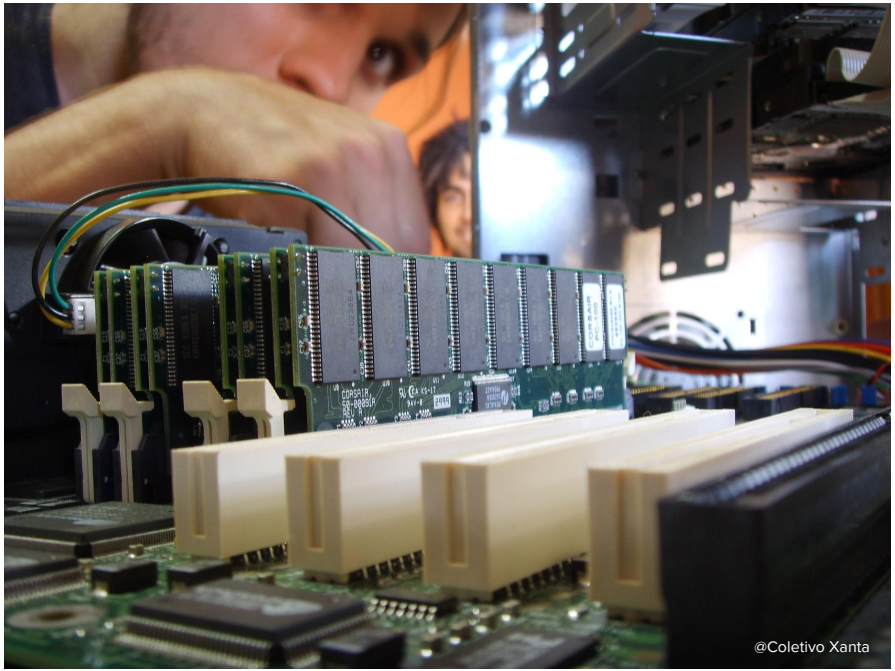
Además de los textos producidos por el Núcleo de Seguridad de la Información de la Escuela de Activismo, invitamos a las personas clave a colaborar con este material, que aquí llamamos Contenido de Apoyo. Son textos que presentan contextos legales, técnicos e históricos de Internet en Brasil. También damos especial atención a la Seguridad Colectiva que sobrepasa las barreras digitales, pero que afecta a los grupos activistas en general.

Estos textos están firmados ya que partieron de una necesidad de la Escuela para producir la Guía. Se encargaron a personas que ya investigan sobre el tema y por lo tanto cuentan con una gran cantidad de información o realizaron una investigación específica sobre ello; por esta razón se les da reconocimiento.

Aunque sean textos de otras personas, te invitamos a interactuar con el contenido, sugerir cambios y colaborar con esa producción. Para una Guía más completa y actualizada, es interesante buscar más artículos y fuentes variadas y ordenar los contenidos establecidos aquí de acuerdo con sus necesidades.

Dado que los contenidos del campo digital están en constante proceso, y por lo tanto en constante actualización, consideramos importante que tengas una base de temas más generales para iniciar, pero que continúes la excavación, la investigación y, siempre que sea posible, te contactes con nosotros para que éste material continúe vivo. Envíanos un correo electrónico con tus actualizaciones para que podamos unirlo a este material en línea.

¡Buena lectura!



EL ESTADO DE VIGILANCIA

Aunque, por una parte, las nuevas tecnologías de la información y la comunicación han traído una potencial forma innovadora para la organización de redes para los activistas, también se ha construido una red de vigilancia masiva sin precedentes. Hoy, Internet puede considerarse una amenaza global para la privacidad.

A lo largo de muchos años, los gobiernos y las empresas han implementado en secreto (o sin el debido escrutinio público) mecanismos de recolección e interceptación de datos. La doctrina de la *guerra cibernética* y la construcción de *cibercomandos* de los militares transformaron el Internet en una herramienta de espionaje sin límites. De esta forma, la capa de la infraestructura global de comunicación y de las nuevas tecnologías está comprometida.

Uno de los más recientes episodios de denuncia de la vigilancia global ocurrió en el 2013, cuando el entonces analista de inteligencia de la Agencia de Seguridad Nacional (NSA) de Estados Unidos, Edward Snowden, filtró miles de documentos a un equipo de periodistas. Los documentos revelaron una profunda red de vigilancia global de espionaje económico y político llevada a cabo por la comunidad de inteligencia del FVEY (Australia, Canadá, Estados Unidos, Gran Bretaña y Nueva Zelanda) contra diversos países, empresas con intereses económicos conflictivos y hasta la Organización de las Naciones (ONU).

Bajo la justificación de proteger a la sociedad contra los "caballeros del apocalipsis de la información" (terrorismo, tráfico de drogas, derechos de autor y pedofilia), los gobiernos y los órganos periféricos de vigilancia, tales como la policía científica, también comenzaron a contratar empresas y servicios *de malware* y de *hacking ofensivo.* Una vez que la comunicación del día a día se incorporó a las aplicaciones, la intervención telefónica solamente ya no es suficiente para las investigaciones penales.

Estas dos tendencias de uso de la red por los gobiernos se refuerzan, en la medida en que la creación de una estructura de vigilancia está justificada para proteger a la sociedad contra un mal mayor. Sin embargo, esta estructura de vigilancia en realidad se utiliza de forma masiva e indiscriminada contra toda la población.

Aunque el poder de la vigilancia global es muy extenso, aún así es posible luchar contra él. El denominado cifrado fuerte, punto a punto, es capaz de impedir que todos sean vigilados. Al utilizar aplicaciones y herramientas encriptadas, o sólo estás protegiendo tu propia comunicación, sino que también estás luchando por el derecho colectivo de privacidad.

Además, es necesario realizar un debate intensivo con los grupos, las organizaciones y la comunidad en general para intentar incorporar la temática de la vigilancia para encontrar posibilidades de apertura y movilidad que incentiven una política de pensamiento que escape de la condición de miedo. Buscar una nueva mentalidad, ligada al sentido de la libertad de actuar y pensar en la red y en el mundo. ▪

Por: Gustavo Gus

LEGISLACIÓN Y VIGILANCIA EN BRASIL

Hay tres leyes principales que tratan cuestiones de monitoreo y vigilancia en Brasil: Ley contra el crimen organizado, Ley antiterrorismo y Ley de intervenciones telefónicas.

En Brasil, tenemos algunas leyes que tratan de prácticas de monitoreo, tales como la intervención de las comunicaciones, el acceso a los datos y la infiltración. Vale la pena destacar las siguientes:

Ley contra el crimen organizado
(Ley N.° 12.850, de 2 de agosto de 2013)

Es una ley del 2013 que modifica el Código Penal y deroga la Ley n.º 9.034/95, y define el concepto de organización delictiva. La ley establece disposiciones sobre la investigación criminal y plantea como medios de obtención de prueba las siguientes prácticas: colaboración premiada; captación ambiental de señales electromagnéticas, ópticas o acústicas; acción controlada; acceso a registros de llamadas telefónicas y telemáticas, a datos catastrales constantes de bancos de datos públicos o privados y a información electoral o comercial; intervención de comunicaciones telefónicas y telemáticas, de conformidad con la legislación específica; el alejamiento del secreto financiero, bancario y fiscal, de conformidad con la legislación específica; la infiltración, por parte de la policía, en actividades de investigación; cooperación entre instituciones y órganos federales, distritales, estatales y municipales en la búsqueda de pruebas e información de interés para la investigación o la persecución criminal.

La Ley contra el crimen organizado hoy en día es uno de los instrumentos más poderosos para la vigilancia y criminalización de movimientos sociales, grupos activistas y disidentes políticos. En octubre de 2013, la Policía Civil de Río de Janeiro llegó a declarar, de acuerdo el diario estatal de San Pablo, que los manifestantes detenidos por actos de vandalismo encuadrarían en la nueva ley. Ya en el 2016, los integrantes del MST pasaron a ser investigados y dos llegaron a ser arrestados, de conformidad con dicha ley, tras la denuncia del Ministerio Público. En el marco de la misma operación, en noviembre del 2016, se enviaron 14 órdenes de prisión preventiva, otras 10 de búsqueda e incautación y 2 más de conducción coercitiva contra integrantes del movimiento en Paraná, en Mato Grosso do Sul y en São Paulo. En esta ocasión, la Escuela Nacional Florestan Fernandes, importante centro de educación y formación de la militancia del MST, fue invadida por policías armados, sin orden judicial. Cuando la ley pasa a ser utilizada como instrumento de criminalización, tales mecanismos se muestran aún más dañinos. En el caso del MST, aunque la investigación se enfoca en un grupo de personas, todo el Movimiento puede estar bajo vigilancia, lo que puede conllevar, por ejemplo, comunicaciones telefónicas y en línea interceptadas y agentes infiltrados.

Ley antiterrorista
(Ley n.º 13.260, de marzo de 2016)

Otra ley preocupante con respecto a su uso para criminalizar movimientos sociales es la Ley n.º 13.260, que tipifica el terrorismo. La ley fue duramente criticada por parte de la sociedad civil brasileña e incluso por la Organización de las Naciones Unidas (ONU). Las principales críticas se refieren al carácter genérico del texto, que puede dar lugar a interpretaciones distorsionadas; al hecho de que la ley estipula sanciones muy severas, y al hecho de que las acciones establecidas en la ley ya poseen tipificación legal en Brasil.
En un pronunciamiento realizado en noviembre del 2015, después de que el proyecto fuera aprobado en el Senado, cuatro ponentes de la ONU manifestaron preocupación por la definición contenida en el texto, que podría "ocasionar ambigüedad y confusión en la determinación de lo que el Estado considera como crimen de terrorismo y podría perjudicar el ejercicio de los derechos humanos y de las libertades fundamentales".

Ley de intervenciones telefónicas
(Ley nº 9.296, del 24 de julio de 1996)

La intervención de comunicaciones en Brasil está regulada por la Ley n.º 9.296/96, que permite la intervención en los sistemas de tecnología de información y teléfonos.

El objetivo establecido por la ley es instruir procedimientos penales o investigaciones. El requisito es una orden judicial, que puede ser emitida directamente por un tribunal o solicitada por las autoridades policiales y por el Ministerio Público.

En líneas generales, la ley estipula que la intervención solo se puede llevar a cabo cuando haya indicios razonables de la autoría o participación en una infracción penal, cuando la prueba no se pueda obtener por otros medios, y cuando el hecho investigado sea un crimen sancionado con reclusión. Sin embargo, en la práctica estos prerequisitos no siempre se respetan. De hecho, este gancho se utiliza muchas veces para iniciar una investigación, como indica el informe final de la CPI con respecto a las intervenciones, del 2007: "La impresión de esta Comisión es que las intervenciones telefónicas se transformaron, así como la confesión en el derecho medieval, en la 'reina de las pruebas', que hace el asunto notorio, manifiesto e incuestionable. Ante las facilidades tecnológicas actuales, intervenir las comunicaciones se ha convertido en una alternativa tentadora, con cierto menosprecio al control legal, en el sentido de que ese debe ser el último medio de prueba que se debe utilizar".

Fuente: Legado Vigilante, un proyecto de Coding Rights

TÉCNICAS DE MONITOREO

Las principales técnicas de monitoreo utilizadas por la policía no son nuevas y ni siquiera son las más sofisticadas. Para resguardarse, son necesarios algunos cuidados básicos de seguridad operacional.

En todas las democracias, los grupos activistas son monitoreados por la policía. No porque sean considerados criminales, sino porque tienen la capacidad de interrumpir el orden. Por lo tanto, no importa si la organización y sus acciones son legales, cualquier grupo o individuo que pretenda cambiar el *status quo* necesita tomar medidas de seguridad. La seguridad del grupo depende del compromiso de cada uno. Por eso, es muy importante realizar procesos de aprendizaje y acompañamiento en ese campo, sea colectivamente, sea individualmente.

El objetivo de la vigilancia es reunir información de inteligencia, es decir, que tiene las llaves de datos que permiten una acción en el futuro. Mientras que antiguamente la policía necesitaba asignar agentes para seguir los pasos de los activistas y subversivos, en la actualidad, con Internet, un solo policía basta en la misión de hacer una "ronda virtual" para navegar por las redes sociales y ver quién son los responsables y articuladores de una determinada protesta.

Para evitar la ronda, es necesario hacer que las acciones estructurales del grupo sean privadas, ya sea fuera de línea o en línea, como las reuniones, encuentros, documentos y conversaciones de la organización. Es necesario evaluar y clasificar qué información es sensible y qué información es pública del grupo. Por ejemplo, si se está planificando una determinada acción no pública, su fecha de realización no debe constar en los documentos públicos del grupo.

Por ejemplo, si se está planificando una determinada acción no pública, su fecha de realización no debe constar en los documentos públicos del grupo. Aunque muchos grupos tienen como principio el libre flujo de información, a fin de evitar jerarquías o desequilibrio de poder, ese mismo principio no puede poner a sus miembros en riesgo. Establecer un proceso de control de la información fortalecerá a su organización a medida que los miembros entiendan cuáles son los riesgos de que un adversario posea cierta información y de lo que tienen que renunciar al revelar determinada información.

La otra técnica que se utiliza es descubrir cómo se organiza el grupo y quiénes son sus miembros activos. Esto se puede realizar, por ejemplo, con investigadores que se hacen pasar por periodistas. Por lo tanto, al dar entrevistas, no digas más de lo que ya es o será público. La rotación de la figura pública puede ser muy útil y, además, una guía de preguntas y respuestas preparadas puede ayudarte a limitar el acceso de los medios a la información del grupo. También es importante, en las actividades públicas, que haya rotación en las funciones.

Por último, si se convierten en un blanco, es posible que se realicen pinchazos y escuchas telefónicas. Al evitar conversar por teléfono sobre la organización o, de ser necesario, utilizando un cifrado P2P, la comunicación estará protegida. Fuera de eso, no hay técnicas para impedir los pinchazos telefónicos. Y es por esa razón que es tan usado por las autoridades policiales. ▪

Por: Gustavo Gus

MOVILIZACIÓN Y BUENAS PRÁCTICAS EN LAS REDES SOCIALES

Utilizar las redes sociales como única herramienta de movilización social puede debilitar a su organización. Mantener canales alternativos no solo es saludable desde el punto de vista de la seguridad, sino que también fortalecerá la lucha.

Actualmente, varias organizaciones han centrado su comunicación en sitios de redes sociales como Facebook, Instagram y Twitter. Aunque pueden tener una gran audiencia en Internet, rivalizando así con la prensa tradicional, desde el punto de vista de la Seguridad de la Información, esas redes crean nuevos riesgos que necesitan atención.

Uno de los principales riesgos al movilizarse por las redes sociales es la generación de diagramas sociales que pueden utilizar los adversarios para el mapeo de su organización y de sus partidarios. Si un observador externo es capaz de conocer las funciones, las personas responsables y el posicionamiento político de cada uno, será capaz de determinar las próximas decisiones de su organización y neutralizar sus acciones.

Además de los diagramas sociales, al concentrar la comunicación en un solo canal, se crea un único punto de falla y, en el caso de las redes sociales, existe un riesgo alto de que la cuenta sea bloqueada o invadida por los atacantes, o suspendida por políticas de moderación poco transparentes. Es también preocupante la ausencia de preservación de la información, ya que es posible que toda la información publicada no sea más accesible en el futuro para su organización. Por lo tanto, además de una buena política de contraseñas seguras y un control de acceso a la administración, siempre deberás tener una copia de la información y también deberás ponerla a disposición en otros canales: blogs, sitios web, otras redes sociales y la propia prensa tradicional.

Es necesario explorar y respaldar alternativas de comunicación e incluir las redes sociales dentro de una estrategia de comunicación. Además de las redes sociales, ¿qué otros canales de comunicación está utilizando su organización? Y aunque las redes sociales tienen una gran audiencia, tener al menos un mailing de sus partidarias y sus partidarios será muy útil en varias ocasiones. ▪

Por: Gustavo Gus

Romerito Pontes | @1º de Maio 2016

[introducción a la seguridad]

Para pensar en la Seguridad, ampliamos nuestros sentidos un poco más allá de la Información, y sugerimos pensar lo que esa palabra significa para cada persona. Es un ejercicio personal, pero que nos ayuda a construir un concepto de la seguridad que se pueda ampliar y que tenga sentido para los grupos activistas de las más diversas áreas. Después de reflexionar, abordamos cuestiones directamente vinculadas con la SI, como el mismo Internet.

¿QUÉ ES LA SEGURIDAD?

El Núcleo de Seguridad de la Información de la Escuela de Activismo viene realizando diversas actividades y estudios con la finalidad de perfeccionar, renovar y construir otros modos de habitar la virtualidad, el Internet, las redes sociales, de lidiar con los medios de comunicación y con el sentido de vigilancia cada vez más difundidos en el país y en el mundo.

En esta caminata de inquietudes y descubrimientos verificamos la necesidad de trabajar con la palabra SEGURIDAD, descubrir lo que había dentro de esta palabra-concepto y llenarla de significados nuevos, más cercanos a lo que veníamos pensando. Se percibe, entonces, una imprescindible necesidad de sentir seguridad en el contemporáneo, algo como una determinación para que la vida sea posible en la sociedad actual. En este sentido, formulamos las siguientes preguntas problematizadoras: ¿Qué es la seguridad? ¿Qué es sentir seguridad?

En una de las actividades de la Escuela, esta pregunta trajo respuestas que nos indicaron lo siguiente:

- Sentirse seguro significa bailar libre en un salón...
- Cuanto más miedo, menos poder. Cuanto menos miedo, más potencia.
- Las soluciones de seguridad son productos exigidos por la sociedad asustada. Es la industria de la seguridad y la producción del miedo social.

Al notar la complejidad y la profundidad de estas preguntas, ya que la seguridad puede ser un sentido, una sensación, una acción o simplemente la profesión de alguien que resguarda la vida de un conjunto de personas, percibimos que sería imposible e incluso poco productivo hacer eso solo con el conjunto de personas de la Escuela. Decidimos, entonces, problematizar este concepto con los grupos con los que actuamos a partir de la Escuela de Activismo ampliando, así, las posibilidades de apertura para nuevos pensamientos a partir de las preguntas y la apertura de posibilidades de más y mayores interlocuciones.

Uno de estos procesos de apertura de este modo de pensar más ampliado ocurrió en la última residencia de Seguridad de la Información de la Escuela, un proceso formativo que involucra a grupos de diversos lugares de Brasil para el intercambio de conocimiento en el campo de la SI.
En el primer día del Encuentro contamos un poco este recorrido y entonces procedimos como se describió arriba: lanzamos las preguntas problematizadoras que tanto nos movieron, junto con la presentación de cada persona que se encontraba allí. El grupo contaba con algunos bolígrafos y tarjetas para responder.

El grupo aceptó el desafío, y con estas preguntas proporcionaron varias líneas. Para algunos, la seguridad recordaba el militarismo, tiempos de un Brasil lleno de prohibiciones y censuras en nombre de la Seguridad Nacional, en favor del orden y del progreso. Para otros, la seguridad recordaba libertad, sentirse a gusto con el propio cuerpo y con los pensamientos. Hubo gente que asoció la seguridad al miedo. Miedo como algo que paraliza, que retira la posibilidad de movimiento, que intercede, interrumpe, que impide a alguien hacer algo.

Y la seguridad como algo inverso al miedo. También hubo quien percibió que la Seguridad es un concepto en disputa y que existe todo un mercado de la seguridad que se organiza a partir del ofrecimiento de más vigilancia sobre los cuerpos. También apareció la seguridad como algo importante para la supervivencia, por eso también está relacionada con la palabra alimentación: seguridad alimentaria.

Muchas palabras fueron surgiendo y asociándose con la palabra-concepto SEGURIDAD. Al final de la conversación, dos palabras aparecieron con bastante intensidad: Control y Límite. Y la idea de la seguridad pública que actúa siempre en esa tensión entre controlar y limitar. El Estado como poseedor del monopolio del uso de la fuerza permitida, y sus mecanismos como las policías de actuación contra los movimientos en el control de manifestaciones. ¿Pero de dónde vienen esos conceptos que se definen jurídicamente? O incluso el mercado, como en el ejemplo de una empresa mundial como Google que, con el propósito de organizar y almacenar datos, tiene acceso a la información que permite un control sobre la vida contemporánea.

Esta actividad fue bastante interesante para nosotros. Hemos podido explorar los pensamientos acerca de la palabra Seguridad y la cantidad de elementos que caben dentro de ella. Nuestra intención con esta sesión era justamente, a partir de esta palabra, descubrir posibilidades de actuación en el sentido de ofrecer más poder y menos temor o miedo. Creemos que este propósito fue alcanzado, ya que el grupo se embarcó en este viaje con nosotros.

Otro aspecto importante fue abrir este concepto con un grupo ampliado, una manera de decir que la Escuela de Activismo no condujo el proceso de aprendizaje por sí misma, pero que quisiera hacerlo sumando las concepciones y opiniones en este campo de luchas allí reunido. El grupo mostró mucha disposición, y la residencia entera transcurrió en ese clima, en ese ejercicio de construcción colectiva y, principalmente, de encontrar posibilidades y resistencias en las luchas. ▪

Algunos textos que se han mencionado para obtener más información sobre los temas:

Deleuze, Gilles. Post-scriptum sobre las sociedades de control.

LECHNER, Norbert. Hay gente que muere de miedo, 2015

Música:
Miedo, de Pedro Guerra / Lenine / Rodney Assis.

SEGURIDAD HOLÍSTICA Y PSICOSOCIAL

En busca del "bienestar en la acción", procura traer más conciencia sobre la seguridad desde una perspectiva de autocuidado y empoderamiento personal y grupal, con base en la percepción de nuestros sentimientos y reacciones y en prácticas de desarrollo de estrategias de seguridad.

La seguridad holística pretende crear estrategias para mantener el bienestar psicosocial de las personas y crear espacios resilientes para el activismo y la resistencia, ya sea trabajando individualmente, en grupos o en organizaciones.

La seguridad es un concepto personal, subjetivo y variable de acuerdo con el género. Debemos tener en cuenta los efectos de diversos tipos de violencia, como la violencia física, estructural, económica, de género, institucional, así como otros tipos de acoso y marginación infundidos por organizaciones privadas, grupos armados, por los Estados y hasta por la propia comunidad o personas cercanas. Estos factores afectan nuestra salud psicológica y física, nuestro bienestar y nuestras relaciones. Tenemos que estar alertas para identificar e implementar estrategias para la seguridad y la protección de nosotros mismos, de las organizaciones de las que formamos parte y también de las personas cercanas.

El enfoque holístico de la seguridad no trata solamente de entender el papel de la dimensión digital en el ámbito personal y político, es decir, de la información electrónica contenida en nuestros dispositivos, bolsillos, mochilas, casas, oficinas, calles y vehículos. También incluye nuestros cuerpos, emociones y estado físico y mental, promoviendo una cultura de cuidados y autocuidados como estrategia subversiva y política de auto preservación, construyendo estrategias de seguridad efectivas.

El enfoque propuesto puede dividirse en tres niveles: seguridad física, seguridad digital y seguridad psicosocial, que deben abordarse como cuestiones integradas. Las estrategias para hacer frente a estas cuestiones se deben revisar constantemente, de la misma manera que el contexto a nuestro alrededor cambia continuamente.

Algunos enfoques de la seguridad holística:
Resistencia y agilidad: A pesar de la importancia de la implementación de planes estratégicos de seguridad, es común que sucedan situaciones inesperadas, y debemos establecer una cultura de autocuidado, presencia y equilibrio mental y emocional para mejorar nuestra capacidad para lidiar con estos eventos. Así, podemos cultivar resiliencia para recuperarnos de los reveses y agilidad para establecer rápidamente nuevas prácticas de seguridad.

Trauma, estrés y fatiga: El estrés y la fatiga pueden llevarnos a identificar y responder mal a los indicadores de amenazas en nuestro medio ambiente. La sobrecarga resultante de los desafíos en nuestras casas, trabajos y vidas y la fatiga generada por trabajar demasiado y durante mucho tiempo sin descanso suficiente hacen que tengamos comportamientos diferentes.

El desarrollo de una cultura (tanto individual y colectiva) de autocuidados y de manejo del estrés es fundamental para un enfoque holístico de la seguridad y el bienestar.

Uso del tiempo: El éxito de una práctica de seguridad depende del buen uso de nuestros recursos, de los cuales el tiempo es uno de los más valiosos a considerar. Como individuos, necesitamos tiempo para reflexionar sobre el efecto que nuestro trabajo tiene en cada uno de nosotros, para elaborar preguntas y buscar respuestas, para identificar tácticas y herramientas para planificar, coordinar e integrar nuevas prácticas en nuestras vidas y trabajo. Debemos construir de manera consciente opciones emocionalmente más saludables y seguras en cuanto al uso de nuestro tiempo.

Por: Foz

MOSAICO DE POSIBILIDADES (MODELO DE AMENAZA)

Somos diferentes, vivimos en diversos contextos y las posibilidades de encontrarnos en situaciones inseguras pueden ser infinitas. El mosaico de posibilidades sirve para trazar acciones más seguras en contextos específicos, sin entrar a la paranoia o inacción ante la complejidad de los riesgos, vulnerabilidades y posibles defensas.

A esta actividad la denominamos "mosaico de posibilidades", pues involucra muchas piezas, herramientas y procedimientos, que, juntos, forman un plan de posibilidades para acciones seguras.

El comienzo del mosaico exige, ante todo, que se prepare la base sobre la cual se montarán las piezas: el contexto. El contexto es algo externo y es aquello en que no podemos interferir, como por ejemplo la criminalización del activismo. Nos muestra las amenazas existentes para una situación o grupo en un momento dado. Es necesario comprenderlo desde múltiples ángulos: político, social, económico, tecnológico y ambiental. La herramienta que mejor aborda esto es el análisis TEPAN (si lo prefieres, puedes llamarlo de PASTEL), una sigla que significa Política (P), Ambiente (A), Sociedad (S), Tecnología (T), Economía (E) y Legal (L). También puedes idear una metodología de acuerdo con la necesidad de su grupo.

A partir de ahí, empezamos a hacer una serie de delimitaciones para definir las vulnerabilidades, como las siguientes:

1) Recursos o activos: todas las personas, programas, aparatos, etc. que son esenciales para que el trabajo se ejecute.
2) Las actividades necesarias para que el grupo realice su misión, como comunicar, organizar, hacer campañas, etc.
3) La información del grupo y dónde está almacenada.

Por medio de estas delimitaciones, analizamos dónde están los puntos débiles que hacen que los riesgos provocados por las amenazas sean más altos y probables.
Para analizar los riesgos, es necesario posicionarlos según su impacto (cuánto daño pueden provocar) y su probabilidad (las posibilidades de que ocurran). Así, sabremos cuáles riesgos son más probables e impactantes y, en consecuencia, dónde debemos enfocar nuestras fuerzas para mejorar nuestras defensas.

CONTEXTO O CASO

Las amenazas pueden ser diferentes de acuerdo con la situación política del país, la represión sobre la causa que defiendes, las tecnologías que se utilizan para monitorear a los activistas, y otros factores.

Un ejemplo: en un contexto donde hay un gobierno opresor, y una persona activista joven va a una manifestación, la amenaza es la criminalización del activismo. Su recurso es el celular, su actividad es comunicar y su información son las articulaciones y los contactos relacionados con la manifestación que están registrados en un chat.

Las posibles vulnerabilidades son muchas: el celular puede no tener contraseña, la persona puede ser estudiante, entre otros aspectos.

Podemos definir algunos riesgos: es posible que la persona sea alcanzada por una bala de goma, vaya presa o que la policía le examine el celular.

Y, analizando esas vulnerabilidades, se llega a la conclusión de que el riesgo de que confisquen el celular es alto y que para disminuirlo, es necesario construir posibilidades como ponerle contraseña al celular, encriptarlo y eliminar vestigios de la articulación de la manifestación.

CONTRASEÑAS SEGURAS

Varios de los servicios seguros que permiten que nuestras vidas estén menos expuestas en el entorno digital requieren una contraseña. En muchos casos, serán su última capa de protección.

En general, cuando queremos proteger algo, usamos una llave para encerrarlo. Las cerraduras de casas, automóviles y bicicletas, todas tienen una clave física. En el entorno digital, las CONTRASEÑAS desempeñan el mismo papel: la tarjetas de banco tienen contraseñas, al igual que las computadoras, las cuentas de correo electrónico, las herramientas, etc.

Estas palabras secretas, frases o secuencias aleatorias suelen ser la primera, y a veces la única, barrera entre la información y alguien que pueda querer leerla, copiarla, modificarla o destruirla sin permiso.

Todas estas llaves, físicas y electrónicas, poseen algo en común: abren los respectivos candados con la misma eficacia independientemente de quien las esté usando, tú u otra persona. Es decir, si su contraseña es débil, o si cae en las manos equivocadas, no va a servir mucho.

Existen varias maneras que se pueden utilizar para descubrir las contraseñas, pero es posible defenderse contra la mayoría con algunas tácticas específicas y el uso de una herramienta de base de datos segura de contraseñas como KeePassX.

¿MI CONTRASEÑA ES SEGURA?

¿UTILIZA LA MISMA CONTRASEÑA EN MÁS DE UN SERVICIO?

SÍ

NO UTILICE LA MISMA CONTRASEÑA EN MÁS DE UN SERVICIO

CONTRASEÑA INSEGURA

NO

¿ES SU FECHA DE NACIMIENTO O DE ALGUIEN DE SU FAMILIA?

SÍ

NO

¿ES UNA PALABRA?

¿ES UNA FRASE?

NO

SÍ

NO

SÍ

ESTA FRASE TIENE SENTIDO PARA ALGUIEN MÁS ALLÁ DE TI?

CONTRASEÑA INSEGURA

TIENE CARACTERES ESPECIALES?

NO

SÍ

CONOCES TU CONTRASEÑA DE MEMORIA?

SÍ

NO

CONTRASEÑA INSEGURA

USTED UTILIZA UN GESTOR DE CONTRASEÑA

NO

SÍ

usted es el tipo de recuperar la contraseña, sí?

SÍ

NO

LA CONTRASEÑA... ÉS SEGURA????

verifique en **howsecureismypassword.net**
pero no escriba su contraseña real

CÓMO FUNCIONA EL INTERNET

La infraestructura del Internet, los protocolos, las tecnologías y los intermediarios detrás del tráfico de información.

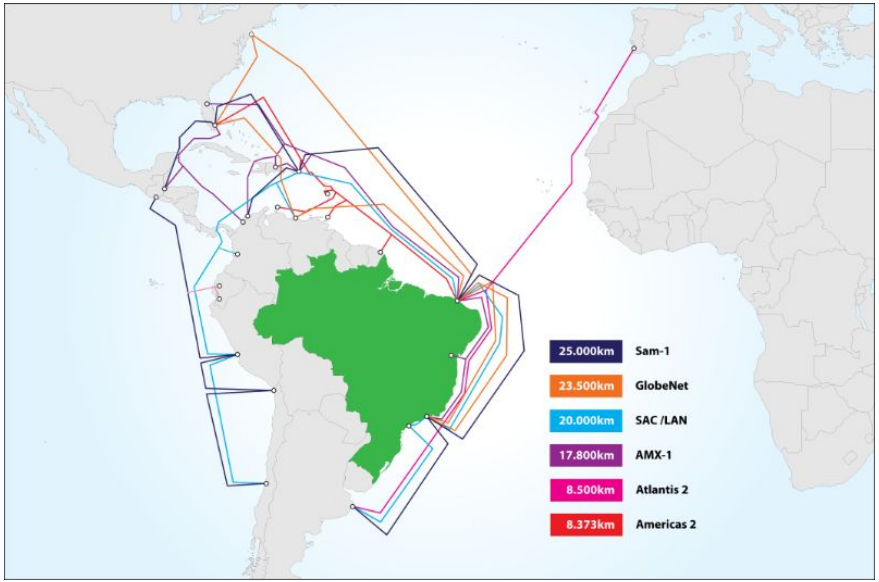
Muchas personas usan Internet todos los días, incluso sin saber cómo funciona. Cuando conversamos con nuestras familias por WhatsApp, enviamos correos electrónicos a amigos y amigas y jugamos en línea, Internet parece una cosa mágica. Y de hecho lo es. La tecnología es magia, y la magia es la tecnología. Pero entender cómo funciona esta magia es muy importante, y es una cuestión política.

Internet es una red de redes interconectadas. De ahí el nombre, inter, de interconectadas, y network, que significa red en inglés. ¡Internetwork! O simplemente, ¡Internet! ¿Pero una red de qué? Internet es una red de ordenadores (¡y personas!), que funciona de forma parecida a un servicio postal. Al igual que el correo, que permite enviar cartas con mensajes y paquetes, Internet permite que los equipos se conecten entre sí para enviar pequeños paquetes de datos que contengan información.

Cuando pensamos en Internet, lo primero que viene a la mente es una nube, ¿verdad? O una imagen muy abstracta. Pero en realidad, Internet es una cosa bien física. Está compuesto esencialmente de cables que pasan por debajo de la tierra (¡y del mar!), y conectan casas, países y continentes. Al conectarte a Internet, te estás conectando a un cable. Es a través de esta infraestructura de cables que se transmiten nuestros pequeños paquetes de datos, de un ordenador a otro. Para conectarse a una página alojada en un servidor en los Estados Unidos, por ejemplo, los datos viajan por los cables, por debajo del mar, hasta el otro continente y, en sólo unos segundos, la página aparece en la pantalla del ordenador.

Para tener una idea, en el mundo actual hay más de 360 cables submarinos en funcionamiento, que alcanzan un total de más de 800 mil kilómetros; si juntáramos todos los cables en uno solo, darían 20 vueltas alrededor de la Tierra. La historia de los cables submarinos es la historia del capitalismo moderno. Desde las Grandes Navegaciones, los europeos se lanzaban al mar para hacer girar la rueda del comercio y acortar las distancias. Pero recién en 1858, con el desarrollo industrial a pleno vapor, comienza a funcionar el primer cable de comunicación transatlántico, construido por los ingleses. Este estaba al servicio de la tecnología en boga de la época: el telégrafo. En los años 1940, con el impulso de la Segunda Guerra Mundial, los cables submarinos fueron modificados para ser usados para la telefonía. El dominio ya no era de los británicos, sino de las empresas estadounidenses. En los años 1980, por fin, surge la tecnología de la fibra óptica, que se comienza a utilizar en los cables submarinos, muchas veces siguiendo las mismas rutas trazadas a finales del siglo 19.

Para que esta maraña de redes, cables y datos funcione, Internet está estructurado a partir de varios protocolos, como veremos a continuación:



Fuente: Francisco Jose Badaro Valente Neto
Cabos Ópticos Submarinos no Brasil - Uma abordagem conceitual

TCP/IP

Para que los ordenadores puedan comunicarse, utilizan una "lengua" común denominada TCP/IP (Protocolo de control de transmisión/Protocolo de Internet). Todo dispositivo (computadora, celular, tablet) conectado a la red recibe un número de IP, para que los dispositivos puedan identificarse entre sí. Para enviar una carta a alguien a través del correo, necesitamos saber la dirección de la persona. Lo mismo sucede en Internet; entonces la IP es un código, un identificador o una dirección.

Cada página en Internet también tiene una IP, para que podamos conectarnos a ellas. Como los números son muy difíciles de memorizar, se ha creado un mecanismo para que podamos identificarlos y acceder a estos a través de direcciones memorizables, es decir, nombres. Si, por un lado, necesitamos saber la dirección de una página para conectarnos a ella, las páginas que accedemos también pueden ver la dirección IP que estamos usando. Pasamos de página en página dejando algunos rastros, y uno de ellos es la dirección IP de nuestros dispositivos.

HTTP y HTTPS

Para acceder a una página, también se utiliza un protocolo de comunicación llamado HTTP (HyperText Transfer Protocol, que en español significa "Protocolo de transferencia de hipertexto"), que es un conjunto de reglas que permiten al ordenador intercambiar información con un servidor que aloja una página. Esto significa que, una vez conectados bajo ese protocolo, los dispositivos pueden recibir y enviar cualquier contenido textual, los códigos que resultan en la página accedida por el navegador (Chrome, Firefox...).

El protocolo HTTP define, entre otras formalidades, cómo se solicitan las páginas web, como se envían los datos que una persona inserta en formularios de inicio de sesión y cómo el servidor envía mensajes de error al navegador del que está accediendo. Sin embargo, como el HTTP es un protocolo basado en texto, es decir, toda la información transmitida está en texto, los datos de una persona que utiliza Internet y el servidor pueden ser interceptados o alterados en el camino.

Esto es porque el HTTP se ha desarrollado para permitir la comunicación, no la privacidad. Como hoy usamos Internet para todo, compartir información, conversar con amigos y amigas, hacer compras y acceder a nuestra cuenta en el banco, la privacidad se ha convertido en una de las cuestiones más importantes.

En ese sentido, se ideó y desarrolló un nuevo protocolo, el HTTPS. Incorpora una capa de protección en la transmisión de datos entre el equipo y el servidor. En las páginas con dirección HTTPS, la comunicación está cifrada, lo que aumenta significativamente la seguridad de los datos.

Es como si el ordenador y el servidor conversaran una lengua que sólo ellos entendieran, lo que dificulta la interceptación de la información.

Al enviar un correo electrónico a una persona, suceden una serie de cosas: primero, conectamos nuestro ordenador a un router a través de una conexión inalámbrica (wi-fi). El router, a su vez, está conectado, a través de un cable, a un proveedor de Internet (Oi, Net, GVT...), que nos da la conexión a la red. Con nuestro ordenador conectado a Internet, el siguiente paso es abrir un navegador (Chrome, Firefox) y acceder a la página de nuestro servidor de correo (Riseup, Gmail, Hotmail...). Allí, escribimos el correo electrónico y enviamos al servidor del correo electrónico del destinatario.

Si nuestro equipo establece una conexión con el servidor de correo electrónico a través del protocolo HTTP, nuestra información viajará a través de la red sin ninguna protección. Sería como si estuviéramos enviando una tarjeta postal, y todas las personas que tuvieran acceso a esta podrían leer el mensaje. Por otro lado, si nuestro equipo establece una conexión HTTPS con el servidor de correo electrónico, nuestro mensaje trae consigo con encriptación entre el equipo y el servidor. Quien determina, en último caso, qué protocolo será utilizado es el servidor, de ahí la importancia de siempre prestar atención si las páginas que visitamos usan HTTPS. Para ello, basta comprobar, en la barra de direcciones del navegador, qué protocolo se está utilizando.

HTTPS también es importante para autenticar la página de acceso. Contiene un certificado que nos permite saber si la página a la que queremos acceder, por ejemplo www.riseup.net, es realmente el grupo Riseup. Esto dificulta que alguien cree una página e intente pasar por Riseup. ▪

VULNERABILIDADES EN INTERNET

La forma en que el Internet está estructurado hoy y la forma en que lo usamos hacen que varios puntos de nuestra conexión y navegación sean vulnerables, y afectan nuestra privacidad.

El router, el proveedor de acceso a Internet y el proveedor de servicios, por ejemplo, guardan información sobre nuestra navegación. Desde el contenido de nuestro correo electrónico, hasta la IP de nuestros dispositivos, el historial de las páginas visitadas, la fecha y la hora que nos conectamos a las páginas de Internet, etc.

Router:
imagina a dos personas con ordenadores conectados a Internet en la misma casa. Una de ellas está actualizando su perfil en una red social, la otra está trabajando. ¿Qué impediría enviar el tráfico de información movilizado por una de ellas a la otra? Dos cosas: las direcciones IP de los dispositivos, y el router. Los routers dirigen el tráfico de Internet, al ayudar a los paquetes de datos a llegar a su destino. Esto significa que toda nuestra navegación pasan por ahí.

Así, quien tenga acceso al router, puede tener acceso a la información de navegación de todos los dispositivos conectados a él. Es por eso que necesitamos configurar los routers que usamos con contraseñas fuertes y protocolos de seguridad. Es por eso también que acceder a los wi-fi públicos puede ser problemático: no es posible saber si hay alguien monitoreando nuestra navegación.

Una forma de evitarlo es prestar siempre atención al tipo de protocolo establecido para acceder a las páginas. HTTPS es siempre más recomendable que HTTP, y hace difícil que terceros conectados al router tengan acceso a nuestra navegación. Otra posibilidad es utilizar servicios y herramientas como VPN (Virtual Private Network) y Tor.

Proveedor de Internet:
los proveedores de Internet son empresas que proporcionan direcciones IP para acceder a Internet, como Oi, Net, GVT. De acuerdo con el Marco Civil de Internet, no pueden bloquear, monitorear, filtrar o analizar el contenido de los paquetes de datos. Sin embargo, el Marco Civil obliga a los proveedores a recoger y almacenar registros de acceso a Internet, que contengan la IP y la fecha y hora de la conexión. Es decir, cada vez que accedemos a Internet, el proveedor que contratamos registra la fecha y hora a la que nos conectamos y desconectamos, y la IP que utilizamos.

Página/Servidor de correo electrónico:
visitar una página es como visitar la casa de alguien, todo lo que haces allí, lo puede ver la dueña de la casa. Además, todas las páginas que visitamos en Internet recopilan y almacenan datos sobre nuestra navegación y dispositivos. Las personas que administran la página de un periódico, por ejemplo, saben a qué hora la IP de tu dispositivo visitó el sitio, en qué enlaces hiciste clic, cuál es el sistema operativo del ordenador, qué navegador se está utilizando, cuál es el tamaño de la pantalla, y mucho más, según la política de privacidad de la página.

Con esta información, logran hasta trazar un perfil de las personas que visitan la página, mostrar publicidades direccionadas, etc.

Un servidor de correo electrónico comercial, como Gmail, Hotmail y Yahoo, además de recopilar toda esta información, también lee todo lo que escribes. A pesar de no cobrar por el uso, ellos ganan dinero con nuestros datos, ya que rastrean y almacenan todos los correos electrónicos, las fotos, los contactos. Saben todo sobre las personas que usan sus servicios y pueden vender estos datos a otras empresas, como las de publicidad, o entregarlos a la policía y agencias de espionaje e Inteligencia.

Para mitigar esta vulnerabilidad, no sirve utilizar HTTPS, ya que el protocolo cifra sólo la conexión entre nuestro ordenador y la página. Esto significa que para una persona externa, interceptar nuestros correos electrónicos puede ser una tarea difícil. Sin embargo, el contenido de nuestras comunicaciones no está restringido solo a los remitentes y destinatarios, sino que también puede acceder quien provee el servicio. Es como si el cartero pudiera abrir y leer todas las cartas que enviamos.

De ahí la importancia de utilizar servicios de correo electrónico confiables y que se preocupen por la privacidad de las personas. Son bastante recomendables los servicios que no poseen como modelo de negocio los datos de las personas usuarias y que por lo tanto no recogen información sobre nuestros dispositivos y no leen nuestros correos electrónicos.

Nube

Cuando accede a una página, en realidad está conectando su computadora a otro equipo, a través de cables y protocolos de comunicación.

Una página se compone de archivos, que "viven" en un servidor conectado a la red. Los servidores no son nubes que flotan en el aire, sino que son ordenadores, conectados a la energía, y ubicados en algún lugar del mundo. Entonces cuando alguien habla de nube, está hablando, en realidad, de una computadora. La nube es siempre la computadora de otra persona. ▪

EL INTERNET QUE QUEREMOS

Ya sabemos cómo funciona el Internet y tenemos bastante contenido para construir nuestro propio Internet, como con las redes malladas. Teniendo en cuenta nuestro contenido y nuestros deseos, **¿cómo es el Internet que queremos?**

Podemos pensar que el Internet es un espacio maravilloso, extraño y muy diverso, con millones de voces, perspectivas y motivaciones que se diferencian y se transforman todos los días. Con eso, hay varias herramientas y varios puntos que podemos analizar y trabajar para construir nuestro propio Internet, más inclusivo, seguro y lúdico.

Presentamos aquí algunas preguntas que pueden inspirarte para pensar el Internet que tú o tu grupo desea:

- ¿El Internet es abierto? ¿Cuáles son los derechos y deberes que tienen las personas, las empresas y los gobiernos tienen sobre este? ¿Hay censura? ¿Los programas son abiertos y accesibles?
- ¿Internet es libre? ¿Todas las personas pueden conectarse a Internet con buena banda ancha y velocidad? ¿El lenguaje de Internet es accesible para todas las personas? ¿Hay seguridad?
- ¿Quién dirige y manda en Internet? ¿Qué leyes y regulaciones que les gustaría a ti y tu grupo que existieran en Internet? En dichas legislaciones, ¿cómo actúan las grandes empresas, los gobiernos, las pequeñas comunidades?
- ¿Siento seguridad cuando utilizo Internet? ¿Cuáles son los riesgos y las vulnerabilidades a las que me expone el uso de Internet? En el Internet que desea, ¿cómo sería la seguridad?
- ¿Hay estándares en el Internet de sus sueños? ¿Todas las personas saben de qué se trata y logran manejarla a primera vista? ¿Cómo funciona la educación en el Internet que queremos? ¿Qué herramientas de aprendizaje activo contiene?
- ¿Qué personas son bienvenidas en el Internet que queremos?
- ¿Quién controla el Internet que queremos?

Más información sobre la salud del Internet.

El único objetivo de estos puntos es inspirarlo, pero hay muchos otros que abundan en el imaginario del Internet: como el propio activismo en sí (un Internet Feminista, Anarquista, Ambientalista, Indígena, Quilombola, entre muchos otros). Lo que proponemos aquí es que tú y tu grupo hagan un ejercicio de imaginación y creatividad, explorando los sentidos, los deseos y las posibilidades de un nuevo Internet. No tengas miedo de cruzar fronteras, ya que como decía un viejo pensador: sin saber que era imposible, fue y lo hizo.

¡Dibuja, garabatea, inspírate!

CÓMO FUNCIONA EL TELÉFONO CELULAR

La estructura del aparato telefónico, la infraestructura de la red telefónica y sus vulnerabilidades.

Esto es lo último que miramos antes de irnos a dormir y lo primera que tocamos al despertar. Los smartphones cambiaron nuestra manera de comunicarnos y también generaron vulnerabilidades que les son propias. Desde la infraestructura a las conexiones virtuales, el teléfono y el smartphone pueden potenciar nuestras voces o callarlas.

Los dispositivos móviles poseen muchos sensores y funciones, y nuestra manera de gestionarlos transforma la seguridad de nuestra información. El número de funciones disponibles en los teléfonos móviles ha crecido en los últimos años, y los aparatos modernos son en realidad miniordenadores portátiles conectados a Internet con funciones de teléfono celular, que pueden incluir la ubicación/GPS, generación y transmisión de archivos multimedia (grabación y transmisión de fotos, vídeo y audio), procesamiento de datos y acceso a Internet, además del tradicional envío de SMS y llamadas telefónicas vía operadora.

Es importante comprender que los teléfonos celulares son inherentemente inseguros:

> La información enviada y almacenada en los teléfonos queda expuesta (almacenada sin cifrar) en los aparatos de origen y de destino de las comunicaciones.

> Para hacer viable el cobro del servicio, el sistema está diseñado para exponer información sobre tu ubicación (a qué antena está conectado el dispositivo) y los metadatos de tus comunicaciones (quién habló con quién y a qué hora).

> La información sobre la ubicación (incluida la ubicación GPS) puede estar incrustada en otros archivos como fotos, mensajes SMS y peticiones de Internet enviadas por el teléfono.

> Las redes de telefonía móvil son privadas y gestionadas por entidades comerciales, y pueden estar bajo el control del gobierno, por diversos motivos (legislación, espionaje, etc).

> Los sistemas operativos usados en los propios dispositivos móviles están desarrollados a medida o configurados por los fabricantes de aparatos telefónicos, según las especificaciones de varios proveedores de servicios y para ser utilizados en las redes de esas mismas empresas. Como resultado, el Sistema Operativo puede tener funciones ocultas para posibilitar un mejor monitoreo por parte del proveedor de servicios de determinado aparato.
Por eso es importante tomar decisiones conscientes al usar teléfonos celulares para que podamos protegernos, proteger a las personas con las que nos comunicamos y nuestra información. La forma en que funcionan las redes y la infraestructura de la telefonía puede afectar de forma significativa la posibilidad de asegurar la privacidad y seguridad de los datos y las comunicaciones.

La estructura básica del celular es la siguiente:

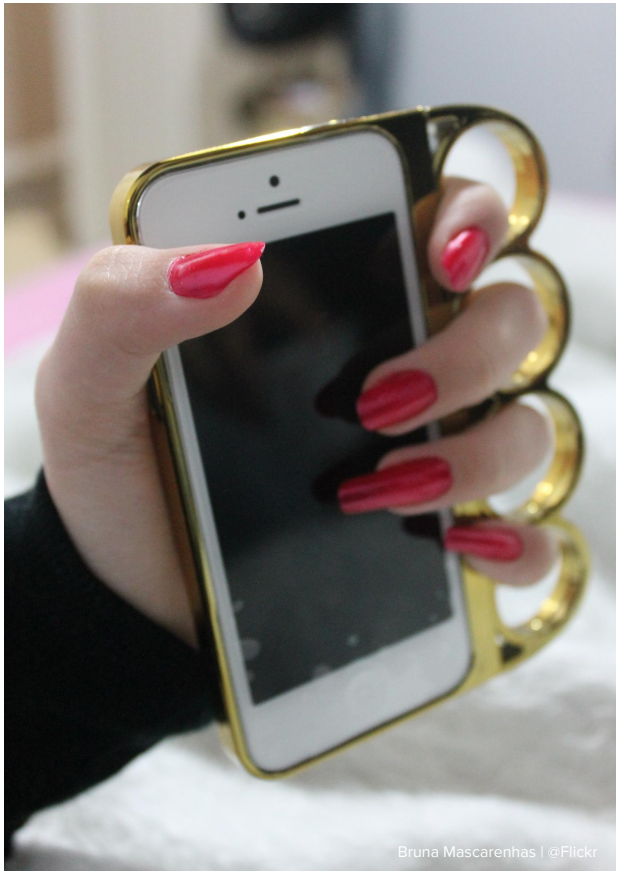
Hardware
Es la combinación de las piezas físicas del aparato.

Firmware
Es el software de base; es decir, que actúa directamente en el hardware, en lugar del sistema operativo.

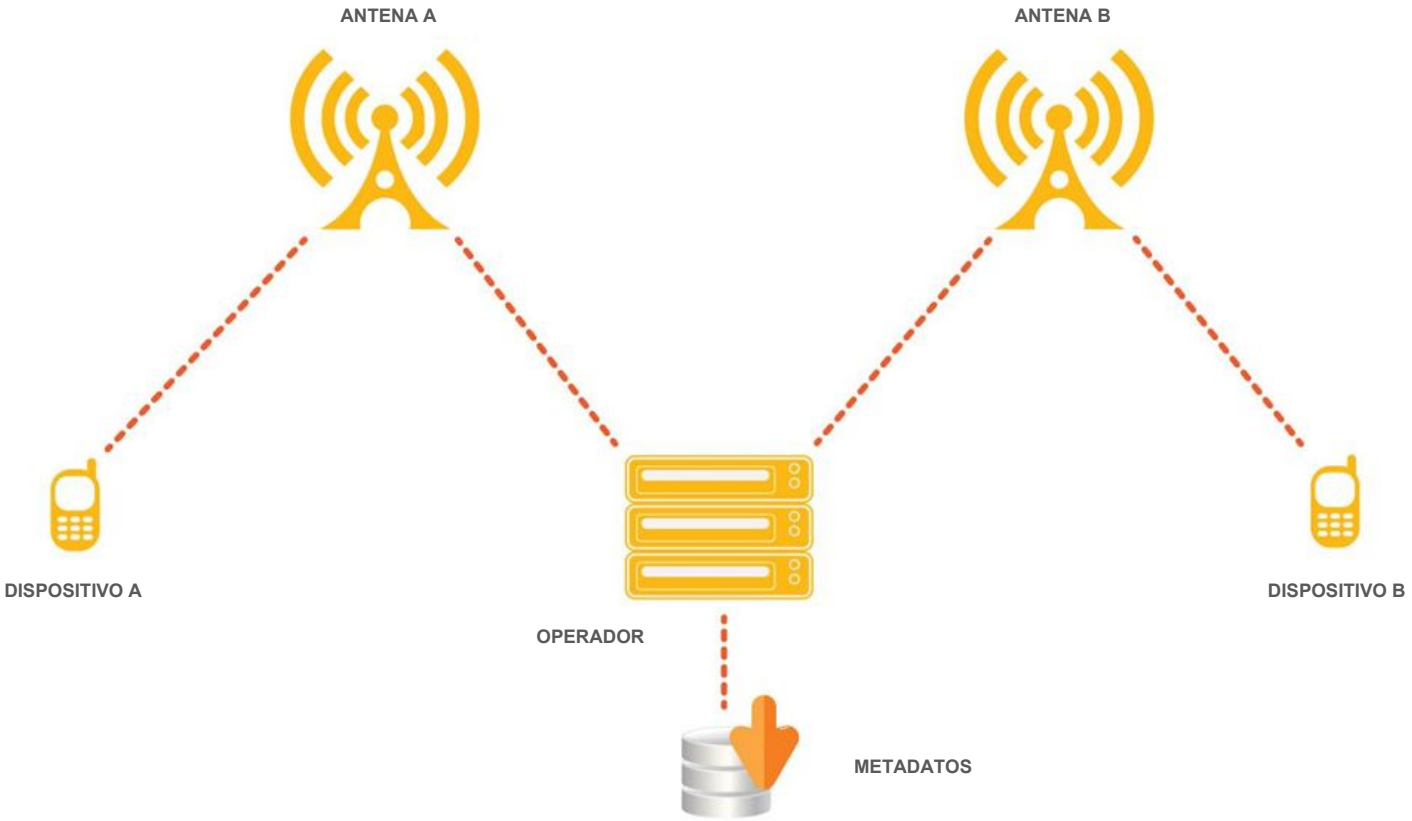
Bootloader
Conjunto de sistemas que permiten la inicialización del aparato; cada dispositivo tiene su propio gestor de arranque.

Módem
Componente propietario esencial para la utilización de las funciones de telefonía móvil.

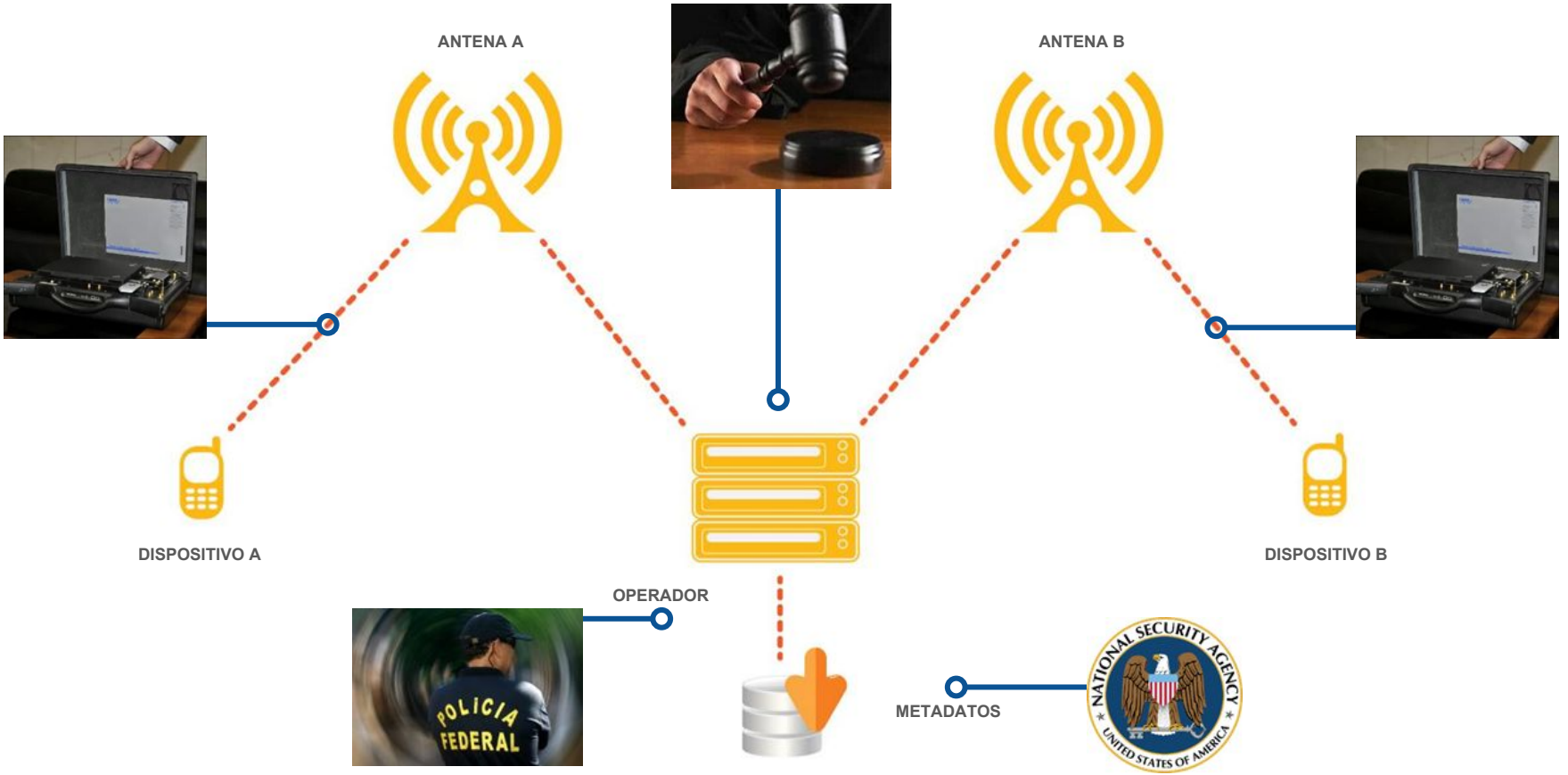
Sistema Operativo
Es el sistema operativo que viene en el celular, o sea, puede ser Android, iOS, Windows, Ubuntu, entre otros.



INFRAESTRUCTURA BÁSICA DE LA RED TELEFÓNICA



VULNERABILIDADES DE LA RED TELEFÓNICA



[amenazas]

Presentamos un conjunto de herramientas y acciones utilizadas por gobiernos, empresas y personas o grupos que intentan rastrear y vigilar datos y actividades de quien sea (activista o no) en Internet, en las comunicaciones telefónicas e incluso en manifestaciones.

15 de abril de 2015
Manifestação - Indígenas de várias regiões do Brasil em frente ao Congresso Nacional.

ENCUENTRA EL P2: P2 es una categoría del servicio de inteligencia de la policía, que también se puede llamar **servicio reservado.** Ese policías andan disfrazados y pueden estar presentes en las manifestaciones, facultades, bares y fiestas del movimiento. ¡Ten cuidado!

Ilustración: Mirim

INFILTRACIÓN: Con el uso de identidades falsas o a través de la corrupción de personas involucradas, agentes de gobiernos o de empresas buscan entrar en grupos activistas como si fueran integrantes, participando en las actividades y conociendo su estructura, para que crear estrategias que, en la mayoría de los casos, generan la dispersión y desmovilización de las actividades de los grupos.

En 2013, con una pluma espiá, una persona infiltrada fue descubierta grabando reuniones del MXVP.

El objetivo seríammonitorear el movimiento hasta desarticular aciones que impidieram el avance de las obras de la Usina Belo Monte

Ilustración: Mirim

*MXVPS = Movimento Xingu Vivo Para Sempre (http://www.xinguvivo.org.br/)

Fuera enviado por la Norte Energia, un grupo de empresas.

El infiltrado hice que la ABIN (Agencia Brasileña de Inteligencia) buscaria con el las informaciones. ABIN afirmó tener una parceria con el grupo de empresas.

El infiltrado el infiltrado accedió a contribuir con las investigaciones e ayudar el movimento, pero después él retrocedió. Su testimonio está en la web.

ESCUCHA

¿CÓMO FUNCIONA?

La intervención de la comunicación, intervención telemática o, más genéricamente, el pinchazo telefónico, es la grabación de la comunicación entre dos o más partes por un atacante. Hay varias formas de intervenir una conversación, sea con grabadores acoplados al cuerpo hasta la intervención en las empresas de telecomunicación. La intervención puede ser un equipo simple, de bajo costo, como un grabador, empleado tanto por detectives privados como oficiales que se dedican a esto, cuando es respaldado por el Estado. Además de los pinchazos telefónicos, las conversaciones en aplicaciones también pueden ser interceptadas. En Brasil, el pinchazo es el principal instrumento de investigación y, aunque está sujeto a una legislación específica, no se limitó su uso masivo, sino que por el contrario, se amplió la colaboración entre el Estado y las empresas de telecomunicación. En el modelo de amenaza del pinchazo, es necesario tener en cuenta que el atacante puede ser la propia parte involucrada en la comunicación.

¿CÓMO PROTEGERSE?

Adopta la siguiente premisa de Seguridad de la Información: si no está cifrada, entonces está intervenida. En el teléfono, no utilices códigos como la sustitución de palabras o palabras clave; los investigadores pueden resolverlos fácilmente. Opta por tratar temas sensibles personalmente en lugar de utilizar medios digitales. Aunque existen equipos telefónicos cifrados, son costosos, y todos los involucrados en la comunicación necesitan tener uno. Una solución más adecuada es utilizar software de llamadas telefónicas con cifrado P2P, como el Signal, y comprobar la identidad de su compañero personalmente.

REFERENCIAS

Grampolandia - La república de la escucha: https://grampo.org

Por: Gustavo Gus

RONDA VIRTUAL

¿CÓMO FUNCIONA?

Imagínate el guardia de ronda de un barrio, siempre al acecho de un acontecimiento inusual. La ronda virtual es como la ronda del barrio, pero ocurre en el ambiente virtual y especialmente en las redes sociales. Pero también existen empresas que prestan este servicio a otras empresas, políticos, etc. ¿Cómo funciona? Es, literalmente, una persona observando TODO lo que usted publica en las redes sociales, lo que usted disfruta y comparte, los eventos a los que usted decide ir, entre otras actividades.

Hay algunos casos de activistas que fueron arrestados, durante escenarios políticos específicos, con el apoyo de investigaciones policiales que utilizan esta técnica de monitoreo. Uno de esos casos ocurrió entre el 2013 y el 2014, en Río de Janeiro, a partir de una investigación policial que llevó a la cárcel a al menos 20 activistas. Con el uso de la ronda virtual, los policías monitorearon las redes sociales y definieron quiénes eran sospechosos según los mensajes, comentarios, fotos, etiquetas y redes de amistad en Facebook.

¿CÓMO PROTEGERSE?

Una de las mejores maneras de protegerse de la ronda virtual estar atento a las configuraciones de privacidad y restringir al máximo el acceso a su perfil y a sus datos (ver más en la sección "Redes sociales más seguras"), especialmente los de las redes sociales.

También es una buena práctica utilizar perfiles diferentes para interacciones y acciones específicas en las redes. Por ejemplo, es posible utilizar un perfil para interacciones más personales, con personas amigas y familiares, y otro perfil para acciones como la administración de páginas o para hacer denuncias. El perfil más personal se puede configurar para priorizar la privacidad, mientras que el otro perfil se puede utilizar con un seudónimo y registrar con un correo electrónico que no sea personal. También se recomienda utilizar la red Tor o VPN para acceder a este perfil para no revelar su IP. Utilizar perfiles con alias y acceder a través de Tor puede causar problemas con Facebook, que tiende a cuestionarlos y borrarlos. Sin embargo, es importante insistir.

Más sobre el tema en:
> Movilización y buenas prácticas en las redes sociales
> *Redes sociales más seguras*
> *Buscador Tor*
> *VPN*

REFERENCIAS

Vigilancia de las comunicaciones por el Estado Brasileño.

RASTROS DIGITALES - METADATOS

¿CÓMO FUNCIONA?

Nosotros generamos metadatos sin saberlo, de una manera ordenada y durante un largo plazo. Conforman la información que acompaña su correo electrónico, su mensaje, sus imágenes/fotografías o algún otro comportamiento suyo en Internet; puede ser información de geolocalización, fecha y hora, autor (el archivo, la fotografía, la aplicación). Y, además, los metadatos facilitan el análisis, el reconocimiento de patrones y las conclusiones sobre quiénes somos y qué estamos haciendo.

Las empresas que están en el centro de nuestras comunicaciones (como los proveedores de telefonía móvil, del servicio de Internet o de correo electrónico) tienen registros detallados de estos metadatos, y eso les proporciona a estas empresas, y a cualquiera que tenga acceso a esa información, un retrato muy preciso de las personas que producen esas huellas digitales.

¿CÓMO PROTEGERSE?

Mantén el control sobre tus dispositivos, lee:
> Cómo funciona el Internet
> Cómo funciona el teléfono móvil
> Programas antimetadatos

REFERENCIAS

Rastros Digitales

BACKDOORS

¿CÓMO FUNCIONA?

Los protocolos técnicos que componen Internet utilizan el concepto de puertos para organizar la comunicación entre los diferentes servicios de la red. Cada servicio puede recibir conexiones en uno o más puertos de entrada. Las *puertas traseras* (o "backdoors" en inglés) son puertas de entrada a algún programa que permiten el acceso a un sistema sin que el usuario o el administrador sepa o tenga control.

Estas puertas traseras se pueden abrir por ataques a fallos de seguridad de un programa o sistema operativo. En estos casos es común que durante el ataque se instalen otros programas (a menudo escondidos o disfrazados de otra cosa) que pueden llegar a dar a la persona atacante acceso total al ordenador afectado.

En otros casos, la puerta trasera se instala deliberadamente, a veces incluso por la fuerza de la ley (véase más abajo el enlace a la historia del *Chip Clipper*).

Es bastante común que las *puertas traseras* permitan el acceso total al software y el hardware del equipo afectado, incluidos los datos almacenados, cámaras y dispositivos USB y DVD, entre otros.

¿CÓMO PROTEGERSE?

Las *puertas traseras* se pueden instalar en un ordenador ejecutando los archivos adjuntos de un correo electrónico infectado o programas descargados de sitios web maliciosos que transportan los virus. Algunas maneras de protegerse de este tipo de ataque son las siguientes:

> No ejecutar programas descargados desde sitios desconocidos, ni adjuntos de correos electrónicos sospechosos.

> Siempre utilizar un antivirus y siempre mantenerlo actualizado.

> Utilizar un *firewall* en los ordenadores funciona como una barrera de las conexiones y puede evitar que un atacante se conecte con *el malware* ya instalado.

REFERENCIAS

Chip Clipper

Guía de autodefensa digital - ordenadores

Seguridad en una caja - Cómo proteger su equipo de ataques maliciosos y hackers

MALWARE

¿CÓMO FUNCIONA?

El malware es un acrónimo de las palabras en inglés *software malicioso* o en español, *programa malicioso.* Es una manera de referirse a la amplia gama de diferentes tipos de programas maliciosos que existen en la web: virus, *spyware, phishing,* troyanos, etc. *Malware,* por definición, siempre tiene algún propósito ulterior. Los ataques pueden pretender robar datos personales, contraseñas, datos bancarios, información sensible, entre otros.

Es posible que el *malware* no esté en ejecución en el ordenador y aún así puede causar daños. En los ataques llamados *phishing,* por ejemplo, un sitio web falso (en un servidor malicioso) puede imitar Facebook, o una página de un banco, o correo electrónico, o cualquier otro sitio que la persona esté acostumbrada a frecuentar, y así robar su datos de acceso.

En otros casos (como los virus/*spyware*/*adware)* el programa malicioso se ejecuta en el mismo equipo de la persona, y la infección puede pasar a través de un programa recibido en un disco duro externo o una memoria USB infectada, o un programa malicioso descargado o un archivo adjunto recibido.

¿CÓMO PROTEGERSE?

Nuestra vulnerabilidad a programas maliciosos depende de cómo nos comportamos como individuos en la web y cómo usamos nuestros dispositivos:

> No abras correos electrónicos y archivos de personas que no conozcas, sobre todo si el asunto del correo electrónico es genérico como "Las fotos de la fiesta quedaron óptimas".

"¿Qué queremos?" "Seguridad en Internet!" "¿Cómo lo queremos?" "Haciendo clic en cualquier enlace e instalando cualquier programa!"

> No utilices un pen-drive y otros dispositivos usb de personas extrañas, y siempre pase un antivirus.

> Mantén tu equipo, tu antivirus y otros programas de precaución siempre actualizados.

> Comprueba siempre que la dirección del sitio al que estás accediendo es la verdadera.

> No hagas clic en vínculos sospechosos.

BIOMETRÍA

¿CÓMO FUNCIONA?

La biometría es la identificación o autenticación de una persona basada en características biológicas únicas, tales como la geometría de la voz, la escritura, la huella digital, el iris, la oreja, la cara o la mano. Por ser una nueva tecnología, se propone como una autenticación más segura. Sin embargo, presenta problemas incluso mayores que otras autenticaciones, como fuga y robo de huellas digitales y otras características personales. Además, si utilizas esta tecnología en tus dispositivos, tales como teléfonos móviles o tabletas, una vez incautados o robados, tus datos estarán disponibles para la autoridad que los capturó.

Un ejemplo de la diferencia de la biometría con las otras maneras de identificación es la contraseña, que una vez creada, se mantiene privada. Además, probablemente también te aseguras de que el número de tu tarjeta de crédito sea privado; sin embargo, en la biometría cualquier persona puede mirarte y ver tu iris o tomar tu huella digital de algo que toques. Es posible que tu cara y tus huellas dactilares ya estén en poder de los bancos de datos de las autoridades. Y una vez que estén en territorio público, cualquier persona puede tomar tu fotografía.

¿CÓMO PROTEGERSE?

En caso de pérdida de contraseñas o de hackeo de tus cuentas con estas, ¿qué tienes que hacer? Cambiar o recuperar tu contraseña, o en caso de pérdida de la tarjeta del banco, cancelarla. Pero si lo hacen con tu huella digital, difícilmente será posible cambiarla. Por lo tanto, la principal recomendación es no utilizar la biometría como su autenticación primaria, ya que no se puede cambiar.

MAN-IN-THE-MIDDLE

¿CÓMO FUNCIONA?

Man-in-the-middle, en español, ataque de intermediario, es un tipo de ataque en el que el atacante logra posicionarse entre las dos partes que se están comunicando e intercepta la comunicación. Para poder realizar esta interceptación, el atacante necesita alcanzar una posición estratégica en alguna red o programa que participe en la comunicación. Una vez interceptada la comunicación, el atacante actúa como un intermediario, haciéndose pasar por cada una de las partes de la comunicación con la otra. Un ejemplo común son las cuentas y facturas falsas en Internet.

Una forma común de *man-in-the-middle* es el uso de *software malicioso* que "secuestra" el navegador de Internet para tener acceso a la información que envíe o reciba a través de él. Otra forma común es la explotación de vulnerabilidades en los routers inalámbricos y la interceptación de la información transmitida a través de estos. Este tipo de práctica tiene resultados más graves pues afecta a más personas, aún más cuando se trata de routers públicos, como en cafés, metros, hoteles, etc.

¿CÓMO PROTEGERSE?

*> Siempre usa una conexión cifrada (con la **S** en HTTP**S**), especialmente para los sitios web donde se necesita ingresar su nombre de usuario y contraseña. Esta tecnología de criptografía tiene como objetivo proteger los datos que viajan y también autenticar el sitio con el que se conecta.*
Utiliza la extensión HTTPS siempre:
https://addons.mozilla.org/pt-BR/firefox/addon/https-everywhere/
https://chrome.google.com/webstore/detail/https-everywhere/

> Mantén tus navegadores y equipos actualizados.

> Utiliza autenticación de dos factores en los sitios web que más frecuentas (como redes sociales) y en los teléfonos móviles.

> No hagas clic en los enlaces de los que desconfías, especialmente los que vienen en los correos electrónicos cuyo remitente no conoces.

HACKING - ATAQUE INTENCIONAL

¿CÓMO FUNCIONA?

Los ataques intencionales de hackers pueden ocurrir de varias maneras: una persona malintencionada que está a tu alrededor, un pariente que quiere descubrir más cosas de tu vida, un hacker que quiere robarte o ataques al azar de hackers con el uso de varios tipos de virus tales como WannaCry. Estos ataques pueden ocurrir de varias maneras: a través de *malwares*, *Man-in-the-middle* o incluso un robo.

¿CÓMO PROTEGERSE?

Hay varias maneras de mantener sus datos y dispositivos más seguros, pero la mejor manera es una combinación de comportamientos seguros.

Para comenzar, se recomienda utilizar un sistema operativo libre como GNU/Linux, que sufre menos ataques de piratería que uno con licencia. Además, mantén tus programas siempre actualizados, especialmente si son actualizaciones de seguridad; también es necesario implementar y mantener contraseñas seguras:

> contraseña de inicio de sesión
> contraseña de administración del sistema
> contraseña de bloqueo de pantalla

Si es posible, utiliza un generador de contraseñas para tener contraseñas más seguras, como KeepassX. Si tienes que utilizar sistemas con licencia, como Windows, siempre recuerde utilizar y actualizar el antivirus, antispyware y bloqueadores de anuncios (se recomienda utilizar el *uBlock Origin).* Es decir, un conjunto de comportamientos, que mitigan la pérdida de datos, mantienen sus dispositivos seguros y actualizan sus copias de seguridad.

PÉRDIDA, ROBO, INCAUTACIÓN O ACCESO JUDICIAL

¿CÓMO FUNCIONA?

Una distracción en un café, una *hora feliz* con los compañeros de la empresa, una tormenta en el camino de vuelta a casa a pie o en bicicleta, así como otros factores, pueden hacer que perdamos nuestros dispositivos electrónicos y digitales que más utilizamos. Ya sea una pérdida accidental o intencional (robo o incautación), puede ocasionar que nos quedemos sin nuestros equipos y, principalmente, sin nuestra información más valiosa. Además, también puede hacer que otras personas sean vulnerables (amigos, familia, trabajo o grupo activista). Por lo tanto, algunas medidas son importantes para mantener los dispositivos seguros.

¿CÓMO PROTEGERSE?

Una combinación de actitudes y comportamientos generales pueden garantizar la seguridad y disponibilidad de tus datos.

>Copia de seguridad encriptada y actualizada;
> Contraseñas seguras;

En el caso de una detención judicial, en la que, probablemente, todos tus equipos serán incautados, te recomendamos que tengas el ordenador encriptado y, posiblemente, una copia de seguridad en una nube o en otro lugar seguro, también cifrada.

REFERENCIAS

Contraseñas seguras

Seguridad en una caja - Cómo proteger tus datos de amenazas físicas

Rosilene Miliotti | FASE

[recursos]

En esta sección, ofrecemos acciones y herramientas para mantener tu vida digital más segura. Recuerda siempre buscar y actualizar la información que ponemos a disposición aquí.

PROGRAMAS ANTIMETADATOS

¿CÓMO FUNCIONA?

Los metadatos son información de un archivo (como un documento de texto, un PDF, una imagen, un archivo de música, etc.) que se almacena en el propio archivo. Esta información puede incluir la hora y fecha en que se creó el archivo, el nombre de usuario de las personas que lo crearon o editaron, información sobre el dispositivo que lo creó y otro tipo de información, como la geolocalización. Como resultado, los metadatos de un archivo pueden decir quién creó el archivo, en qué equipo o dispositivo, cuando y en qué localidad. Los programas antimetadatos, básicamente, eliminan toda la información (o la información seleccionada) de un archivo determinado.

¿CÓMO PROTEGERSE?

Puedes comprobar los metadatos de una foto haciéndole clic con el botón derecho del ratón y seleccionando Propiedades o utilizando un software de visualización de metadatos, como Photome. Además, es posible evitar que un tipo específico de metadatos, como la localización GPS, sea capturado:

> Apaga la ubicación inalámbrica y GPS (en servicios de localización) y los datos móviles (esto se puede encontrar en el gestor de datos -> entrega de datos).

> Al tomar una foto, asegúrate de que la configuración de la ubicación de la etiqueta de la aplicación de fotos también está deshabilitada.

Si deseas eliminar el metadato de varios archivos, puedes utilizar programas específicos como Metanull (quita metadatos de imágenes en Windows) o MAT, que elimina metadatos de varios tipos de archivos.

REFERENCIAS

Eliminación de metadatos (inglés)
Programa antimetadatos de linux - MAT

NAVEGADOR TOR

¿QUÉ ES?

El Navegador Tor es un programa de software libre y de código abierto, diseñado para permitir el anonimato en línea y para burlar la censura. Funciona en una gran red de miles de servidores, administrados por personas voluntarias de todo el mundo. Para hacer una nueva conexión, selecciona tres de estos servidores, llamados transmisiones Tor, y se conecta a Internet a través de ellos. Se cifra cada parte de ese trayecto, de modo que no sepan a dónde se envían y reciben los datos.

Al usar el navegador Tor, tu tráfico en Internet aparecerá en una dirección IP diferente, generalmente de otro país. Como consecuencia, el Navegador Tor oculta tu dirección IP de los sitios a los que accedes, así como oculta tales accesos a terceros que intentan monitorear tu tráfico. El navegador también garantiza que ninguna transmisión Tor pueda revelar al mismo tiempo tu ubicación en Internet y los sitios que visitas, aunque algunos de ellos (sitios o terceros) reconocen uno u otro.

¿CÓMO USARLO?

El Navegador Tor está disponible para GNU Linux, Mac OS, Microsoft Windows y sistemas operativos de Android. Para usarlo en tu computadora, solo tienes que instalarlo a través de la página del Proyecto Tor (enlace abajo). Y para usar en el celular, es necesaria la combinación de dos aplicaciones: Orbot (para habilitar la red Tor) y Orfox (para iniciar el navegador anónimo y seguro).

REFERENCIAS

Navegador Tor para Windows
Proyecto Tor
Orbot y Orfox

¿CÓMO FUNCIONA?

Técnicamente, para acceder a una página en línea, necesitas que tu proveedor de Internet (ISP) conecte su dispositivo al servidor web de la página. El proveedor necesita saber la IP (o dirección) de la página que deseas acceder para que pueda hacer la conexión; es decir, el proveedor sabe qué páginas está accediendo. Sin embargo, si estás en un país que censura Internet, el proveedor consultará una lista de sitios prohibidos y entonces decidirá si debe o no hacer la conexión.

Además, las páginas también pueden ver quién se conecta a ellas a través de las IP de nuestros dispositivos. Así, cuando accedes a una página, al mismo tiempo, le informas al proveedor de Internet la IP de la página y le informas a la página la IP de tu dispositivo. Esto sucede, en realidad, con gran parte de los servicios en línea que accedemos, no sólo con páginas.

Para no caer en la censura o para proteger tu privacidad mientras navegas por Internet, puedes utilizar una VPN *(Red Privada Virtual).*

Una *Virtual Privacy Network* o *Red Privada* Virtual es un servicio que conecta el dispositivo a otro dispositivo a través de una conexión cifrada. Así, todo el tráfico de tu red pasa primero por este dispositivo, y luego va a Internet. Esto significa que ni su proveedor de Internet puede ver a qué servicios está accediendo, ni los servicios pueden ver su dirección IP. La VPN enmascara su dirección IP y parece que está en otro lugar, lo que evita así la censura y la exposición. Además, encripta toda tu conexión.

Pero ATENCIÓN: el dispositivo intermediario puede ver todo tu tráfico, lo que hace que no toda la VPN sea confiable.

¿QUÉ VPN USAR?

Recomendamos algunas VPN:

> La VPN del grupo Riseup
> La VPN del grupo Autistici/Inventati
> La VPN del grupo AktiviX - para usarla, tienes que solictarlo por correo electrónico
> Esta no es activista y es paga, pero es segura, Acceso privado a internet

CORREO ELECTRÓNICO SEGURO

¿CÓMO FUNCIONA?

Si ya sabes *cómo funciona el Internet*, también sabes que nuestra información básica de metadatos circula en el Internet y por el proveedor y el servidor de correo electrónico. Un servicio de correo electrónico seguro es el que se compromete a no acceder a tus correos electrónicos, venderlos o brindar tu información personal y de metadatos a terceros. Los correos electrónicos tradicionales, sean los de grandes multinacionales o de pequeñas empresas, no suelen ofrecer este tipo de protección, además de que algunos exigen métodos de identificación personal (copia de RG, etc.). Un servidor de correo electrónico seguro, además de garantizar tu anonimato, también proporcionará una conexión encriptada y, si es posible, encriptará tu buzón de correos electrónicos. Estos servicios, en general, son mantenidos por grupos y personas que creen en un Internet libre y abierto, que actúan contra la censura y a favor de un mundo distinto, más accesible.

RECOMENDADOS

Algunos servidores (activistas) proporcionan correos electrónicos seguros. Como los costos para mantener los servidores de correo electrónico son altos, restringen el uso a grupos de personas y activistas de confianza. Conoce algunos:

> *Riseup.net - debe tener una invitación para registrarse; pedir a alguien que tenga cuenta allí.*

> *Autistici.org - una pequeña pero sincera presentación puede garantizarte un correo electrónico seguro.*

> *Resist.ca - un formulario para saber más ti y tus principios te puede garantizar o no una cuenta en este servidor activista.*

KEEPASSX

¿QUÉ ES?

KeePassX es una herramienta que te permite almacenar y administrar múltiples contraseñas dentro de un archivo de base de datos cifrado. Este archivo se cifra con una contraseña maestra que tu creas. KeePassX también se puede utilizar para generar contraseñas fuertes para tus cuentas a través de parámetros definidos por ti.

Como la base de datos generada por este se cifra, puedes almacenar copias en varios lugares, lo que hace que la copia de seguridad de tus contraseñas sea relativamente simple. No recomendamos enviar tu base de datos por correo electrónico o almacenarlo en línea donde otras personas podrían tener acceso. Muchos usuarios de KeePassX mantienen una copia en su ordenador principal, una copia en un dispositivo USB y una copia en su disco de copia de seguridad.

CÓMO USARLO

KeePassX está disponible para GNU Linux, Windows y Mac OS X. Puedes descargarlo directamente desde el sitio o desde tu gestor de paquetes si utilizas GNU Linux o Mac OS X. Al iniciar KeePassX debes crear una nueva base de datos (será un archivo guardado en tu computadora o donde tú prefieras) que puede contener tus contraseñas personales, contraseñas de trabajo, o cualquier otra cosa. Esta base de datos se puede definir a través de categorías (correo electrónico, sitios, compras, servidor, etc.) donde se puede registrar tu nombre de usuario, tu contraseña, algún consejo, entre otras cosas. Además, puedes copiar tu contraseña directamente desde tu base de datos, sin necesariamente verla.

REFERENCIAS

> Como instalar KeePassX

> Como hacer y mantener contraseñas seguras

REUNIONES EN GRUPO EN LÍNEA Y SEGURAS

¿CÓMO FUNCIONA?

Para hacer reuniones o conferencias en línea con múltiples personas a través de audio y chat seguros, es posible usar los programas Jitsi o Mumble, dos programas libres y de código abierto que tienen encriptación P2P y que funcionan en Windows, Linux y OS. Existen también proveedores del servicio Jitsi en línea (Jitsi Meet), que no requieren instalación de software.

Jitsi es una herramienta para videoconferencia que proporciona cifrado P2P para conversaciones de voz (ZRTP sobre SIP). Su uso más común es a través de servicios en línea, organizados por el mismo Jisti o por Greenhost. Con ellos, es posible crear salas seguras para las conversaciones sin tener que instalar nada, directamente desde el navegador de Internet. Solo tienes que crear una sala y pasar la dirección de acceso a otras personas, que también podrán acceder a esta desde sus navegadores. Para aquellos que dependen del celular, la aplicación Jitsi Meet busca simplificar este acceso.

Mumble es una herramienta de audioconferencia, sin soporte de vídeo, que se puede utilizar para reuniones entre dos o más personas. Es necesario instalar el programa o la aplicación móvil (Plumble para Android y Mumble para iOS) y utilizar el servidor estándar de Murmur. También puedes instalarlo en un servidor adecuado. Mumble se conecta a través de TLS y el audio se encripta con AES. Además, permite la autenticación por contraseña para los usuarios.

OTRAS FUNCIONALIDADES

La versión instalable de Jitsi también se puede utilizar como un programa de mensajería segura (messenger). Como Jitsi es compatible con Facebook Messenger y con otros protocolos populares de telefonía (Jabber/XMPP, AIM, ICQ, MSN, Yahoo! Messenger y SIP), basta con configurarlo para usar tus cuentas ya existentes. En este caso, el beneficio es poder proteger las conversaciones de texto usando el protocolo OTR (Off-the-Record), de encriptación P2P.

El contenido de tu comunicación pasa a ser inaccesible para terceros, tales como el gobierno o plataformas de vigilancia corporativas, además del propio servicio de intercambio de mensajes, si estás usando Facebook Messenger, Facebook; si estás usando Google Talk, Google.

REDES MALLADAS

¿CÓMO FUNCIONA?

Las "redes malladas" son redes informáticas distribuidas. En los últimos años, se ha popularizado el concepto de redes autónomas (o redes libres) como la infraestructura alternativa de una comunidad. Las redes autónomas se construyen en un barrio, un pueblo/aldea o una ciudad, normalmente por los propios habitantes, en un proceso colaborativo. Son muy populares en áreas carentes de infraestructura y pueden o no proveer acceso a Internet. Sus principales características son las siguientes:

> Estructura distribuida. El crecimiento es posible desde cualquier punto;
> Respeta la neutralidad de la red;
> La comunidad debe tener autonomía para mantener su red y sus servicios sin el apoyo de empresas.

CONSIDERACIONES SOBRE SEGURIDAD

Utilizar servicios locales de red como chat, telefonía e intercambio de archivos evita que tu información fluya por la red de empresas y gobiernos. Esta autonomía atrae a comunidades preocupadas por la privacidad a invertir en infraestructura propia administrada por personas de confianza. A pesar de ello, se debe mantener el uso de criptografía fuerte y demás prácticas de seguridad holística, pues siempre es posible que personas infiltradas accedan a esa red y expongan información vulnerable de los demás usuarios.

REFERENCIAS

Proyecto Rizoma de Redes Libres - la posibilidad de crear una infraestructura de comunicación popular que sea abierta, descentralizada y gestionada por sus propios usuarios

Introducción a Redes Autónomas del Grupo Vedetas

Wiki de la documentación de Coolab

MENSAJERÍA SEGURA

¿CÓMO FUNCIONA?

Hay muchas aplicaciones de comunicación asincrónica, es decir, mensajes que se pueden recibir incluso si una de las partes está sin conexión o no está disponible. Estas son algunas aplicaciones de este tipo de comunicación: WhatsApp, Signal, Telegram, Threema, Viber, Wire. Aunque algunos de ellos prometen la seguridad y privacidad de las comunicaciones de sus usuarios, hay algunas decisiones y especificaciones que deben tenerse en cuenta al optar por utilizarlos. La primera de ellas es si el software de la aplicación y el código que se ejecuta en el servidor es abierto/libre o cerrado/propietario. Esto significa que si en el caso del software de propietario, no es sencillo saber cómo funciona su seguridad. La segunda es que no basta con saber si es cifrado, sino que también es necesario conocer cuál es el tipo de criptografía utilizada y si sigue las buenas prácticas del área. La tercera cuestión es lo que la empresa o la organización responsable hizo en el pasado al ser solicitada para entregar los datos de sus usuarios a las autoridades (de cualquier país). La cuarta cuestión es conocer el modelo de negocio de la aplicación: si no vende los datos del usuario, ¿cómo paga las cuentas? ¿Existirá en el futuro o es solo una startup?

¿CÓMO PROTEGERSE?

No exponga información sensible en aplicaciones sin encriptación P2P en ninguna situación. Signal es desarrollado por WhisperSystems y tiene la mejor evaluación al realizar las preguntas anteriores. Es recomendado por expertos del área de la Seguridad de la Información como, por ejemplo, Edward Snowden, exanalista de inteligencia de la NSA. Si un contacto utiliza medios no cifrados para iniciar una conversación, dile a esta persona que hable contigo en Signal. Recuerda habilitar los mensajes efímeros para que los mensajes se borren después de un período y evita acumular muchos historiales de conversaciones. Siempre verifica personalmente la identidad de tus contactos. Es un proceso rápido y que alertará cualquier cambio de la identidad de tu contacto.

REFERENCIAS

Campaña “Usa Tor, Usa Signal”

Por: Gustavo Gus

COPIA DE SEGURIDAD

¿QUÉ ES?

El backup es una copia de seguridad de los datos almacenados en tus dispositivos, como documentos, fotos, contactos, entre otros. Hay varias maneras de hacer esta copia de seguridad: puedes configurar un programa para realizar una copia de seguridad de forma rutinaria, o puedes realizarla manualmente, al copiar y transferir los datos de un dispositivo a otro. El objetivo es que usted se resguarde de una posible pérdida de archivos originales, ya sea por acciones desproporcionadas como perder un celular, pendrive o por tener un problema con su disco duro, por la incautación de los equipos, o por un mal funcionamiento de los sistemas. Tener una copia de seguridad permite restaurar los datos perdidos.

¿COMO HACER?

La copia de seguridad se puede realizar en archivos guardados en el equipo, en el teléfono y en la tableta, pero lo ideal es almacenar copias en dispositivos diferentes para asegurarse de que no se pierdan. No recomendamos usa la nube (Dropbox, Google Drive) para copias de seguridad, a menos que mantengas tu propia nube y, además, que tus datos estén cifrados. Recomendamos, además, que el dispositivo de la copia de seguridad esté cifrado para asegurarte de que los terceros no tengan acceso.

REFERENCIAS

Cómo recuperarse de la pérdida de información

SAFER NUDES - ENVÍA NUDES

¿CÓMO FUNCIONA?

En tiempos de "porno de venganza" (*Revenge Porn*), saber cómo enviar nudes es fundamental. El proyecto Safer Nudes fue iniciado por la organización Coding Rights para abordar el debate sobre la privacidad en línea de una manera divertida. Es una guía que defiende el derecho de hacer y enviar nudes como "una práctica de resistencia placentera contra el machismo, el conservadurismo, el racismo y la heteronormatividad". Por lo tanto, "publicarlas o no debe ser una elección exclusivamente tuya, en el ejercicio de tu derecho a la privacidad".

CONSEJOS

Safer Nudes es una guía sensual en formato de revista, con instrucciones para protegerse al enviar tus fotos. Algunos consejos:

> Anonimiza

> Utiliza canales seguros a la hora de compartir.

> Utiliza contraseñas fuertes en tus redes.

> ¡No muestres tu cara o marcas/tatuajes que pueden identificarte en las fotos!

¡Acceda a la revista y obtén más consejos!

REFERENCIAS

Safer Nudes

CÓMO HACER UNA DENUNCIA DE FORMA SEGURA

LA IMPORTANCIA DE DENUNCIAR

Tenemos que lidiar, dentro y fuera de contextos activistas y de movimientos sociales, con diferentes tipos de violencia: acoso moral y sexual, abuso de poder, robo, violación, persecución física y virtual, persecución policial, intimidación, entre otros. Esta violencia tiene que ver con las estructuras de poder establecidas en las relaciones entre las personas en esos diferentes contextos. Una denuncia de un caso de violencia puede ser una herramienta para reorganizar esas relaciones de poder. Entre los objetivos finales de la denuncia están el bienestar de la persona denunciante, la responsabilización de la persona denunciada y la ampliación de la reflexión y conciencia en la comunidad involucrada, generando potencial para cambios.

RIESGOS INVOLUCRADOS

El éxito de una denuncia depende de diversos factores, como la efectividad de las personas e instituciones involucradas en la recepción y procesamiento de la denuncia, el estado emocional y preparación previa de la persona denunciante, y el nivel de influencia y poder de la persona denunciada. La preparación de una denuncia debe tener estos factores en cuenta para ampliar la seguridad física, mental y emocional de la persona denunciante.
La violencia que genera la necesidad de denuncia impacta en la integridad física y mental de la persona denunciante, que a menudo ya llega bastante frágil en los momentos de decisión y elaboración de la denuncia. Un proceso de denuncia realizado sin la debida atención puede empeorar la situación de quien denuncia. El apoyo físico y psicológico puede ser fundamental para garantizar el bienestar de la persona denunciante.

DENUNCIA ANÓNIMA

En ciertos casos, puede tener sentido denunciar de forma anónima. Algunos órganos e instituciones incluso tienen políticas para ello. En estos casos, es importante contextualizar lo que se entiende por anonimato para garantizar que se logren los efectos pretendidos y minimizar los posibles efectos colaterales resultantes de la falta de información.

El acto de denuncia puede dejar rastros, ya sea al hacerla personalmente, por teléfono, carta o Internet. Si es importante que tu identidad permanezca oculta, detente un momento a pensar de qué formas es posible minimizar los rastros. Algunos elementos a tener en cuenta son la presencia de cámaras de seguridad, los registros de llamadas telefónicas (no sólo de los números de los aparatos, sino también de las torres de teléfono y horarios de las conexiones), la posibilidad de grabación y del uso de técnicas de reconocimiento facial y de voz, los registros de datos de navegación en Internet, etc.

También existe un equilibrio entre la credibilidad y el anonimato. El hecho de ocultar la información de autoría suele, irónicamente, tener efectos opuestos en las denuncias reales y falsas. Por un lado, es importante que una denuncia anónima real sea lo más precisa y completa posible para compensar la ocultación de la autoría. Pero, por otro, también es importante evitar detalles que puedan acabar revelando la identidad de la persona denunciante.

FORMAS DE DENUNCIAR

Hay varios canales "oficiales" para realizar denuncias en línea, tanto del Estado como de grandes empresas, ONG y hasta grupos autónomos. Tú puedes hacer una búsqueda para averiguar cuál es el canal adecuado para hacer una denuncia. En casos de publicaciones no autorizadas o amenazas en línea, muchos sitios proporcionan medios para solicitar la eliminación de contenidos explícitos o difamatorios.

Es importante conocer, también, formas alternativas de denunciar cuando los medios oficiales no son suficientes. Las manifestaciones artísticas y los escrachos, por ejemplo, son formas no institucionalizadas que encontraron algunas personas para hacer su denuncia más efectiva.

Busca el apoyo de personas cercanas y de confianza. Entrar en contacto con grupos especializados también puede ser una buena forma de ampararse durante el proceso de la denuncia. Contacta a tus grupos de confianza más cercanos, como grupos de mujeres, LGBT, grupos técnicos que trabajen con Seguridad de la Información, etc.

Para denuncias anónimas en Internet puedes utilizar el Navegador Tor o Tails. Lee sobre el anonimato en línea para no cometer errores comunes. Evita utilizar correos electrónicos comerciales o redes sociales, ya que son más vulnerables al monitoreo.

Tal vez tu proceso de denuncia implique la necesidad de una acción judicial. Para obtener información acerca de un defensor público, marca 129.

Para denuncias de violencia contra mujeres, marca 180.

Para denuncias de violencia, abuso sexual, abuso físico o psicológico contra niños y adolescentes, denuncias de personas en situación de calle, de las personas LGBT, personas con discapacidad y de la tercera edad, marca 100.

REDES SOCIALES MÁS SEGURAS

¿CÓMO FUNCIONA?

Las plataformas de socialización en Internet nos permiten articular, gestionar y mover a nuestros grupos de manera más práctica, pero también implican varios problemas relacionados con la seguridad y la privacidad. Además de construir una gran minería de nuestras redes más cercanas y de nuestros contactos, tales plataformas a menudo venden nuestros datos a grandes empresas. Nuestra comunicación, cuando se encuentra en un estado de exclusión, puede ser interceptada legalmente.

Por lo menos, lo que podemos hacer es enfocar nuestra protección a través de la concientización de la estructura de privacidad que esas redes nos permiten.

Configurar tu línea de tiempo de manera que sólo las personas amigas puedan ver tus publicaciones personales, y de manera que nadie pueda postear en ella además de ti. Configura las opciones de etiquetas en las publicaciones y las fotos de manera que puedas analizar y elegir antes de que las etiquetas se puedan publicar. Esto evita que los contenidos sensibles (como redes de amigos, ubicación, información sobre la familia) estén disponibles para cualquier persona. Además, verifica siempre en tus redes sociales:

> ¿Quién puede ver mis publicaciones?
> ¿Quién puede ver mi perfil?
> ¿Quién puede ponerse en contacto conmigo?
> ¿Qué aplicaciones están autorizadas o vinculadas a mi red social?

Ver también el tema Mensajería Segura

Cómo protegerse y mantener tus datos seguros al usar los servicios de las redes sociales

REFERENCIAS

Configuración de seguridad para redes sociales

Orgía de datos: el swing sin el consentimiento de las aplicaciones de encuentros

[referencias]

Esta guía no sería posible sin el uso de varios materiales que están disponibles en Internet, realizados por grupos comprometidos con el Internet libre y la antivigilancia. Hemos reunido una serie de enlaces se consultaron y, algunas veces, modificaron para este material. En ellos podrás encontrar más información, y profundizar tu conocimiento. ¡Disfruta!

Laísa Mendes | @Porto Alegre

REFERENCIAS Y OTROS ENLACES RECOMENDADOS

Guía práctica para combatir la vigilancia en Internet:
http://www.temboinalinha.org/

Guía práctica de estrategia y tácticas para la seguridad digital feminista:
http://feminismo.org.br/guia/guia-pratica-seguranca-cfemea.pdf
Guía para enviar nudes de manera segura:
https://www.codingrights.org/safernudes/

Guía de autodefensa digital:
https://autodefesa.fluxo.info/

Herramientas de seguridad digital para todas las personas:
https://securityinabox.org/pt/

Guía de seguridad para ir a protestas:
http://protestos.org/

Yo y mi sombra - Asuma el control de sus rastros: https://myshadow.org/pt
Videos - Introducción a la privacidad:
https://vrr.im/9d

Juego para encontrar infiltrados, de Pública:
http://apublica.org/vigilancia/infiltrados/

Estrellas - Servidora feminista para grupos feministas:
https://vedetas.org/

Manual de seguridad para defensores de derechos humanos en riesgo:
https://www.frontlinedefenders.org/pt/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk

Acortador de enlaces feministas y seguros
https://vrr.im/

CryptoRave - 24 h de actividades, talleres y fiestas sobre la encriptación:
https://cryptorave.org/

Lavits - Red latinoamericana de estudios sobre vigilancia, tecnología y sociedad:
http://lavits.org/?lang=pt

Principios para un Internet feminista -
https://www.genderit.org/sites/default/upload/fpi_v3.pdf

Cl4ndestina - Servidor feminista:
https://clandestina.io

Taller antivigilancia:
https://antivigilancia.org/pt/boletim-11-pt/

Escuela de Activismo:
https://ativismo.org.br

Agradecemos a Graciela Selaimen por su fuerte apoyo al campo de la defensa de derechos.