

Diagnósticos en seguridad digital para organizaciones defensoras de derechos humanos y del territorio: un manual para facilitadores



(/wiki/index.php/File:01_ManualSD_TR.png)

Índice

- 1 Presentando el manual
 - 1.1 ¿Por qué es necesaria la mirada tecnopolítica?
 - 1.2 Las miradas feministas
 - 1.3 La educación popular
- 2 ¿Cómo usar esta guía?
- 3 Preparativos
- 4 Investigación
 - 4.1 Materiales útiles
 - 4.2 Planificación y comunicación de la agenda
 - 4.3 Planificación del viaje
- 5 Cuidado colectivo
 - 5.1 Equipo de facilitación
- 6 Día 1
 - 6.1 Trabajo colectivo
 - 6.1.1 Presentación
 - 6.1.2 Actividad: Dibujar mi día al lado de la tecnología
 - 6.1.3 Actividad: ¿Qué información se produce?
 - 6.1.4 Actividad: Lluvia de actores
 - 6.1.5 Actividad: Acotando actores
 - 6.1.6 Actividad: El semáforo de la información
 - 6.1.7 Actividad: Puertas y candados para la información
 - 6.1.8 Comentarios de cierre del trabajo colectivo
 - 6.2 Análisis del ambiente físico y de los equipos de cómputo
- 7 Evaluación del día y revisión de archivos
- 8 Día 2
 - 8.1 Conclusión del análisis de equipos de cómputo y redacción del informe preliminar
 - 8.2 Presentación del informe preliminar
- 9 Diagnóstico final
- 10 Recursos útiles
- 11 Agradecimientos
- 12 Créditos
- 13 Anexo I
- 14 Versión en inglés
- 15 Referencias

Presentando el manual



(/wiki/index.php/File:24_ManualSD_TR.png)

En la mitología griega, Dedalus era un creador de artefactos, sus obras mostraban constantemente el profundo conflicto entre la innovación y su uso como herramienta del poder o la ambición. Como si fuese uno más de los artefactos de Dedalus, entre los sueños utópicos y las pesadillas, la tecnología actual no ha logrado escapar de sus propias paradojas. En el sueño de Dedalus, la innovación tecnológica serviría para volar y escapar del encierro pero en ese impulso humano de quedar cegado ante lo luminoso y la posibilidad, Ícaro, su hijo, llevó al límite el sueño.

Actualmente, la tecnología sigue jugando este papel: en el sueño potencia nuestra libertad y bienestar, pero se juega siempre en el límite. En el caso de las tecnologías de la información y la comunicación (TIC), como en la mitología, éstas nos dan la posibilidad de buscar la libertad traspasando fronteras, combatiendo discursos dominantes de odio, dando espacios para lo diverso, el encontrarnos y reconocernos, el compartir. Sin embargo, atadas a sus propias vulnerabilidades, las TIC exponen a quienes las usamos a riesgos como la vigilancia, el espionaje e incluso la manipulación.

El trabajo de los y las defensoras de los derechos humanos y del territorio, sin duda, se ha beneficiado del desarrollo de nuevas tecnologías para actividades importantes como comunicarnos, generar campañas, compartir información, hacer análisis, documentar casos y guardar datos. Al mismo tiempo, el uso de la tecnología ha generado nuevas vulnerabilidades, evidenciadas por eventos documentados, entre ellos: la infección de computadoras por autoridades gubernamentales con programas para vigilar, compra de equipos para monitorear llamadas, robo de computadoras a organizaciones sociales, pérdida/robo del celular con información personal y de trabajo que después se expuso en redes sociales, espionaje sobre redes sociales e intrusión en cuentas de correo o facebook.

La información que comúnmente nos llega sobre la capacidad de vigilancia que podría tener el Estado, algún cartel e incluso particulares, usando la tecnología, puede exacerbar el miedo y fomentar la autocensura. Puede parecer que solo hay dos opciones extremas: o usa la tecnología sin protección porque no hay nada que puedas hacer o destruyamos la tecnología. En la práctica, esta disyuntiva se reduce a la decisión de usarla o no.

Nosotras abogamos por una postura distinta, que no parte de la desesperación, ni de responder con violencia, sino con auto-determinación: si bien la tecnología no es ni el principio ni el final del problema, un uso consciente puede potenciar nuestras acciones, evitar o mitigar vulnerabilidades y ayudar al cuidado colectivo.

A partir de nuestra propia experiencia dentro de colectivos, trabajo con organizaciones muy diversas e investigación, creemos que es importante generar estrategias y sumar a los análisis de seguridad de las organizaciones lo que se conoce como seguridad digital; que implica analizar nuestro uso de la tecnología, entender nuestras vulnerabilidades, encontrar herramientas que nos sean oportunas y desarrollar capacidades internas para integrarla dentro de un esquema general de seguridad.

Desafortunadamente, las organizaciones y colectivos, debido a problemas como la falta de tiempo, recursos o conocimientos, pocas veces cuentan con la oportunidad de generar esta integración de la seguridad digital como un proceso. Esto resulta frecuentemente en que al final las medidas acordadas se abandonan con el tiempo.

Desde las comunidades técnicas que tienen un compromiso social, existe también una dificultad para contribuir en estos procesos, ya que en muchos casos, si bien los conocimientos sobre seguridad digital pueden ser sólidos, la falta de estrategias pedagógicas o de experiencia sobre las condiciones reales en las que se desarrolla el trabajo cotidiano de las organizaciones, se crea una barrera que impide la comunicación y la transferencia de conocimientos.

Para que un proceso de seguridad digital sea apropiado efectivamente por las organizaciones, es fundamental que el conocimiento no se integre desde las voces expertas, sino desde el compartir y recrear. El paso inicial de tal proceso es el diagnóstico participativo.

En este manual, las **Técnicas Rudas** presentamos una propuesta metodológica para implementar diagnósticos de seguridad digital para organizaciones que trabajan en la defensa de los derechos humanos y/o del territorio. Este manual está dirigido especialmente a talleristas, facilitadores y expertos en seguridad digital que trabajen con organizaciones sociales. Sin embargo, creemos que puede ser útil para guiar a una organización que decida iniciar el proceso por sí misma.

La propuesta se caracteriza porque tiene una postura tecnopolítica e introduce una mirada feminista. En consecuencia, se basa en la educación popular como herramienta pedagógica.

¿Por qué es necesaria la mirada tecnopolítica?

De forma superficial, el debate sobre las vulnerabilidades limita las consecuencias en el ámbito de la privacidad individual, generando una respuesta particularizada que se reduce a frases como "no tengo nada que ocultar", que no logra integrar el alcance social que estas tienen. Mientras que los especialistas buscan soluciones reduccionistas, como el que una aplicación se encargue de **parchar vulnerabilidades**.



(/wiki/index.php/File:03_ManualSD_TR.png)

Sin embargo, un análisis más profundo sobre la tecnología, da cuenta de cómo en las diferentes fases de los procesos tecnológicos existe una visión

política-económica. Así, al momento de ser construida, se hace evidente la necesidad de analizar de dónde se obtienen los minerales indispensables para sus componentes, las manos de quienes trabajaron para su producción, las condiciones laborales; en dónde es producida y cómo llega a los mercados, el cómo estas mercancías serán consumidas, cruzadas por el género y la clase. Y al final serán desechadas bajo un esquema territorial del planeta, impuesto desde un porcentaje pequeño de la población que acumula la riqueza.

Esta mirada profunda que identificamos como tecnopolítica, ha hecho evidente que existe un interés económico en la obtención de datos personales a partir del uso de medios digitales. Por ejemplo, se puede ver la investigación de Coding Rights (<https://chupadados.codingrights.org/es/>).

También han sido expuestas evidencias de vigilancia local y global. Por ejemplo, al momento de escribir este manual, en México se han mostrado evidencias de espionaje a periodistas y organizaciones defensoras de derechos humanos usando el software Pegasus^[1].

Para la región, en 2015, filtraciones de correos de la empresa Hacking Team evidenciaron la enorme inversión que gobiernos latinoamericanos habían hecho en hardware y software para la vigilancia^[2].

Sobre vigilancia masiva, el caso más conocido fue el de las filtraciones (https://en.wikipedia.org/wiki/Global_surveillance_disclosures_%282013%E2%80%93present%29) hechas por Edward Snowden en 2013, que mostraron un elaborado aparato de vigilancia global operada por la NSA (National Security Agency por sus siglas en inglés) de Estados Unidos^[3].

Considerando las condiciones sociales es importante alertar a quienes defienden los derechos humanos y el territorio que usan las TIC para sus comunicaciones, incluso como parte de sus estrategias de lucha, sobre sus vulnerabilidades.

La seguridad digital requiere una mirada tecnopolítica porque solo podrá responder certeramente a los retos actuales siendo sensible a las condiciones reales en las que las personas las usamos.

En la práctica, estas consideraciones se traducen en optar por software libre (ya que es transparente en su código y da la posibilidad de enriquecerlo), evitar contribuir en el desecho de tecnología o caer en el juego de la obsolescencia programada y tener prácticas pedagógicas que consideren aspectos sociales.

Las miradas feministas



(/wiki/index.php/File:04_ManualSD_TR.png)

Partimos de que no existe un feminismo, existen múltiples feminismos. Entre ellos, está el Transhackfeminismo que, si bien no cuenta con una definición clara (y probablemente no pretenda nunca una definición estática), rescata cuatro aspectos básicos:

a) El prefijo trans que hace referencia a la transformación, transgresión, transitoriedad; es el cambio y el saltar fronteras.

b) Hack, que en sus orígenes tiene que ver con trabajo mecánico que se repite. Es esa gota de agua que de tanto caer traspasa todo, es la esencia de Marie Curie procesando una tonelada de *Pechblenda* para obtener un gramo del material que le permitió descubrir el radio.

c) El feminismo como estas múltiples formas que han dado cuenta de cómo este sistema que sobrepone el capital a lo humano y ha basado su crecimiento en la explotación del cuerpo de la mujer, invisibiliza trabajos esenciales para la reproducción de la vida humana, discrimina y crea fracturas en las comunidades.

d) Desde la América Latina, **la gran Abya Yala**, sumamos los feminismos comunitarios que introducen un ecofeminismo ligado a la tierra y descoloniza la mirada.

Desde el transhackfeminismo es posible ubicar la asimetría que hay para acceder al conocimiento y generar estrategias. Pone en el centro la comunalidad como nuestra base; cuestiona y desactiva las prácticas de poder al compartir conocimiento.

La educación popular



(/wiki/index.php/File:05_ManualSD_TR.png)

Existen una gran variedad de prácticas pedagógicas en manuales de seguridad digital, en algunos casos sólo son recomendaciones sobre dinámicas, útiles, por ejemplo, para despertar a los participantes cuando están cansados, algunas otras van más lejos y emplean técnicas de educación para adultos. Nosotras decidimos trabajar a partir de la educación popular^[4], porque compartimos que:

a) Educar es un acto político en el que existen relaciones de poder y hay que romper con esos esquemas.

b) Creemos que la teoría y la práctica están dialécticamente relacionadas.

c) Como lo dice la etimología de la palabra: la conciencia proviene del conocimiento aprendido con otros/as.

d) Asumimos que *el mundo no es, el mundo está siendo* (Paulo Freire).

¿Cómo usar esta guía?



Esta guía está enfocada en la comunidad de entrenadores o facilitadores en seguridad digital, pero también puede ser útil para una organización que ha tomado la decisión de iniciar su proceso de seguridad digital por sí misma. La estructura y las actividades propuestas pueden y deben adaptarse a las circunstancias y necesidades específicas de la organización. La guía también puede ser una referencia útil para los facilitadores cuando llevan a cabo el diagnóstico de una organización o grupo. La metodología también puede aplicarse a evaluaciones individuales con ajustes mínimos.

Preparativos



(/wiki/index.php/File:06_ManualSD_TR.png)

Considerando que el diagnóstico contempla tanto actividades in situ como trabajo de gabinete, para tener una facilitación eficiente y segura es vital estar preparado. Lo que significa:

1. Entender el contexto tecnopolítico en el que se desenvuelve la organización.
2. Proveer a la organización de una explicación precisa de cómo se llevará a cabo el diagnóstico, su propósito y las expectativas sobre los miembros de la organización que participen.
3. Estar seguro que se cuenta con todos los insumos materiales necesarios.

A continuación damos una serie de ideas de cómo prepararse, pero es importante que cada paso sea asimilado en su esencia y tratar de adaptar de forma creativa las situaciones particulares.

Investigación



(/wiki/index.php/File:26_ManualSD_TR.png)

a) Conociendo a la organización.

Tal vez la invitación a colaborar llegó por la conexión de una persona cercana y por transferencia de confianza se tienen premisas tácitas. Sin embargo, tanto para evaluar el riesgo para el equipo de facilitación como para el proceso de diagnóstico, es necesario ampliar lo más posible este conocimiento, investigar quiénes son y lo que trabajan.

Hay que tomar en cuenta que la idea no es hacer un análisis invasivo, convertirse en stalkers (<https://en.wikipedia.org/wiki/Stalking>)^[5] o exponer a las organizaciones en su vulnerabilidad, porque esto podría crear desconfianza, incomodar a la organización o poner a los/las participantes a la defensiva. Es necesario ser sensibles y tener claridad en el límite de la búsqueda de información pública. De ser necesario, durante el trabajo *in situ* se pueden aportar mecanismos sobre cómo hilar entre los diferentes tipos de información pública que existen y la información que, sin estar totalmente pública, las empresas que se utilizan para servicios como correo electrónico o redes sociales, pueden tener y combinar para diferentes tipos de análisis.

Consideramos información pública necesaria para esta primera aproximación toda la que esté disponible en prensa, comunicados políticos, la que se encuentre en redes sociales, la que esté disponible en su sitio web (incluyendo información sobre el servidor en el que se aloja, el representante legal y técnico que se asocian al dominio y sus

direcciones oficiales, la cual se obtiene fácilmente a partir de páginas como <https://whois.net/default.aspx> (<https://whois.net/default.aspx>) y, si es posible, quien provee el servicio de correo electrónico.

A partir de esta información, se trata de contestar preguntas como: ¿Qué temas se abordan? ¿Quiénes podrían estar interesados en oponerse a este trabajo o a quiénes afecta este trabajo? ¿Qué tan públicas son las personas que trabajan en la organización? ¿Con qué otras personas o instituciones se les puede asociar? ¿En qué país se encuentra el servidor de su sitio web? ¿Cuál es la información personal identificable (IPI^[6]) del personal dentro de todos los datos que se han encontrado? ¿Es posible ubicar geográficamente las instalaciones de la organización? ¿Se pueden conseguir teléfonos de las oficinas o sitios de trabajo y teléfonos personales? ¿Han tenido incidentes de seguridad o amenazas reportadas públicamente?

b) Análisis del contexto tecnopolítico regional, nacional y local.

Esto incluye conocer y relacionar las temáticas que trabaja la organización y las posturas que habría sobre las mismas a nivel gubernamental nacional, estatal y local. Es importante buscar si se han reportado indicios de compra de equipos o asociación con empresas dedicadas al espionaje o la vigilancia y si ha sido una práctica gubernamental documentada la represión o la vigilancia. También se puede buscar la trayectoria de gente que participe del gobierno local/estatal/nacional.

Asimismo, es relevante investigar marcos normativos que permiten la vigilancia, entender bajo qué causales se permiten y qué instituciones específicas pueden ejercerla. Si no existen reportes, tal vez es necesario llevar a cabo solicitudes de acceso a la información si se cuenta con ese mecanismo en el país en el que se trabaja.

c) Actualización sobre programas y herramientas.

Esto incluye conocer sobre equipos y software dedicados al espionaje (torres falsas de celular -IMSI catchers-, aplicaciones, bloqueadores de señal, aplicaciones que explotan vulnerabilidades), sus costos, funcionamiento y facilidad para obtenerlos.

También es útil que se conozca a las compañías y sus políticas de privacidad, así como las capas de seguridad de sus programas y fallos reportados para:

- Correo electrónico
- Servicios en línea (archivar y compartir documentos, calendarios, construcción de escritos colaborativos en tiempo real, etc.)
- Programas que se utilizan comúnmente para dar soporte en línea
- Redes sociales
- Sistemas operativos comunes

Materiales útiles

Para la sesión de análisis participativa: Lápiz de cera, rollos de papel kraft (https://es.wikipedia.org/wiki/Papel_de_estraza), plumones, marcadores para pizarrón, hojas tamaño carta, estambre o hilo grueso de colores. Etiquetas redondas de colores (verde, amarillo, rojo, azul), tijeras (si se viajará en avión hay que recordar ponerlas en el equipaje que no va en cabina o las perderán).

Para los diagnósticos de las computadoras:



(wiki/index.php/File:08_ManualSD_TR.png)

- Al menos dos memorias usb totalmente limpias. Si se han usado con anterioridad hay que asegurarse de no solo de borrar los datos, sino de reescribir sobre ellos antes de usarlas.
- Versiones en vivo^[7] de antivirus (por ejemplo: ESET SysRescue y AVIRA).
- Versión en vivo de un sistema operativo GNU-Linux.

Para el segundo día debes asegurar que puedes imprimir el reporte preliminar.

Planificación y comunicación de la agenda

Descartando el tiempo dedicado a los preparativos, la fase de análisis y redacción del informe final; la metodología de diagnóstico que proponemos requiere dos días seguidos de trabajo in situ. Idealmente son 16 horas en las oficinas de la organización pero el equipo de facilitación debe estar preparado para destinar un poco más de tiempo durante esos días.

Tal vez una pregunta que salta es por qué dos días. Es el tiempo promedio máximo que, en nuestra experiencia, una organización puede inicialmente comprometerse para dedicar al proceso.

Dependiendo de cómo esté estructurada la organización, para el diagnóstico es crucial que participe al menos un miembro de cada área/equipo de trabajo. Esto debe quedar bien claro en la comunicación con la organización, ya que es frecuente que sólo se cite al personal que da mantenimiento a las computadoras y/o directivos. La intención de convocar al menos a una persona de cada área/equipo es tener una muestra lo más real posible de cómo cotidianamente se trabaja.

La forma en la que recomendamos que se reparta la agenda dentro de los horarios de oficina es:

Primer día

- Sesión matutina conjunta para un análisis de riesgos, guiada por dos personas del equipo de facilitación (aproximadamente 4 horas), una tercera persona se ocupará de iniciar el diagnóstico de los equipos de cómputo (estimamos que se invierten 20 minutos aproximadamente por equipo. En las siguientes secciones daremos más detalles).
- Sesión vespertina para evaluar computadoras (4-6 horas).

Para la noche del primer día, es necesario que el equipo de facilitación se reúna para hacer una valuación de la sesión matutina y un primer análisis de hallazgos, confirmar agenda y prioridades para el siguiente día.

Segundo día

- Sesión matutina para concluir la revisión de los equipos de cómputo (4 horas aproximadamente).
- Redacción del reporte preliminar (2 horas).
- Sesión vespertina para presentar el reporte preliminar y la retroalimentación del mismo (2 horas).

Los detalles sobre cada actividad se presentarán en las siguientes secciones.

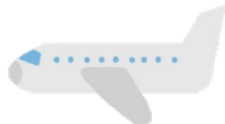


(/wiki/index.php/File:09_ManualSD_TR.png)

Es muy importante comunicar de forma clara todas las actividades a desarrollar, tiempo esperado y personal de la organización que es requerido para las sesiones conjuntas, así como las necesidades y tiempos para el

diagnóstico de los equipos de cómputo.

Planificación del viaje



(/wiki/index.php/File:10_ManualSD_TR.png)

La planificación del viaje se debe hacer contemplando presupuesto, evaluación de seguridad, condiciones para un buen descanso (tal vez toca

dormir poco pero hay que poder dormir bien) y condiciones adecuadas para trabajo nocturno.

Sobrepasa los objetivos del presente manual hacer una descripción detallada sobre los cuatro aspectos; sin embargo, hay algunos recursos en línea que pueden ser de utilidad para orientarse (hemos puesto algunos en la sección de Referencias útiles).

Es necesario asegurar que toda la logística es correcta, como la dirección del lugar donde se llevará a cabo el diagnóstico, tener un número y persona de contacto, prever el tiempo y medio de transporte local y coordinar la entrada y salida de las oficinas, para estimar el tiempo que requerirá evaluar los equipos de cómputo y el ambiente físico.

Cuidado colectivo

Una buena atmósfera de trabajo parte de la generación de espacios seguros, en los que existe un ambiente positivo de trabajo, se cuida de maximizar los niveles de energía y dedicación, tanto de las personas participantes como del equipo de facilitación.

Algunos preparativos que puedes considerar para el cuidado colectivo son:

1. Incluir como parte del servicio de café, fruta de temporada y agua.



(/wiki/index.php/File:11_ManualSD_TR.png)



(/wiki/index.php/File:12_ManualSD_TR.png)

2. Es muy útil llevar semillas o alimentos que proveen energía para que el equipo de facilitación pueda consumir en momentos breves.
3. Es importante estar atentos de los/as participantes y de los/as integrantes del equipo de facilitación para poder detenerse a descansar en algunos momentos, aunque no estén en la agenda, o sugerir alguna dinámica energizante.

Equipo de facilitación

En nuestra experiencia, el equipo ideal está compuesto por tres personas por cada 8-12 participantes. Lo que se busca es contar con personas que cubran los siguientes aspectos:

- Conocimiento en el análisis de las computadoras y herramientas de seguridad digital.
- Conocimiento en técnicas pedagógicas.
- Capacidad de investigación.
- Trabajo en el tema de cuidados o acompañamiento psicológico a comunidades con estrés.

Es común que no se pueda contar con el equipo ideal. En su defecto, hay que tratar de apoyarse en recursos sobre el tema y que por cada facilitador no haya más de diez personas.

Si el equipo está compuesto por biohombres y biomujeres, es importante ser consciente que la tendencia en el trabajo con organizaciones es dar mayor peso a la palabra masculina en los aspectos técnicos o tal vez también pueden existir otras características dentro del equipo de facilitación que despierten asimetrías. Por lo tanto, es primordial tomar conciencia de los privilegios sociales que se le pueden atribuir a los diferentes miembros del equipo y tratar de mitigar prácticas jerarquizantes.

Día 1



(/wiki/index.php/File:13_ManualSD_TR.png)

El trabajo in situ para el primer día se divide en dos partes: el trabajo colectivo y el inicio de la revisión de los equipos de cómputo y del ambiente físico.

Trabajo colectivo



(/wiki/index.php/File:07_ManualSD_TR.png)

Es necesario llegar con anticipación para preparar el espacio de trabajo. Antes de iniciar la sesión:

- Colocar las sillas y las mesas en forma de medio círculo.
- Poner lápices de cera de colores y/o plumones y hojas en el centro de la mesa.
- Recortar y pegar tres columnas de papel kraft o estraza (https://es.wikipedia.org/wiki/Papel_de_estraza) sobre una pared visible para todos/as; estos deben ser tan largos como el equipo de facilitación alcance a escribir sobre de ellos.
- Recortar y pegar otra columna de papel kraft separada para el glosario.
- Pedir las contraseñas de internet por si es necesario investigar algo en el momento.

Presentación

Tiempo estimado: 10 minutos

La sesión inicia con una breve dinámica de presentación del equipo de facilitación y de los/as asistentes. En este punto se provee información sobre el equipo de facilitación así como de lo que se espera del diagnóstico. Se puede aprovechar para enfatizar que en el diagnóstico no hay respuestas buenas o respuestas malas, sino que hay lo que se hace, así, sin calificativos. Es primordial ser muy sensible para detectar si existe algún tipo de resistencia o temor por parte de algún participante, para verbalizarlo y hacer notar que el diagnóstico no es una evaluación hacia las personas, sino que busca conocer qué se hace y con qué se hace para sugerir un plan apropiado de seguridad digital. También hay que destacar que el equipo de facilitación sólo pretende ayudar a ir generando el diagnóstico pero que se parte del conocimiento que los/las participantes tienen, por lo que es indispensable su participación.

También como parte de la presentación es importante hacer acuerdos de formas de trabajo. En educación popular usamos:

- Forma es fondo
- La memoria es más extensa que la inteligencia.
- La memoria colectiva es más extensa que la memoria individual
- La letra con juego entra
- Nadie aprende en cabeza ajena
- Entre todos/as sabemos todo
- Nadie libera a nadie, nadie se libera solo. Nadie educa a nadie y nadie se educa solo
- Evitar negar a el/la compañero/a.
- Sumar la idea de el/la otro/a.
- Escucha activa
- Evitar calificativos
- Evitar monopolizar la palabra
- Para hacer más fructífera la discusión, ir sumando, no redundando en lo dicho
- No imponer ideas

Actividad: Dibujar mi día al lado de la tecnología

Tiempo estimado: 45 minutos

Objetivo: Conocer dispositivos, programas, aplicaciones que se usan y para qué se usan. Este ejercicio permite también conocer si los mismos dispositivos son usados para trabajo o actividades personales.

Descripción: Se pide a los/las asistentes que dibujen su día al lado de las tecnologías que ocupan (no sólo las de trabajo sino las que usan cotidianamente; por ejemplo, aplicaciones biométricas o de esparcimiento, como las de citas o sitios de taxi). Hay que mencionar que con esta actividad se busca una narrativa, así que para las personas que no se sienten tan cómodas dibujando, pueden escribir un texto.

Sugerencia: Antes de iniciar las presentaciones de los dibujos, podría ser útil dividir la primera columna del papel kraft en cuatro secciones: "Celular", "Computadora", "Celular+Computadora" y "Otros dispositivos", para apuntar los usos de la tecnología bajo el tipo de dispositivo que más le corresponde.

Posteriormente, cada participante describe su dibujo. Mientras lo hace, un miembro del equipo de facilitación va apuntando en la primera columna de papel kraft los "Usos de la tecnología" que debe reflejar el dispositivo/aplicación y su uso, por ejemplo:

- Yo uso la alarma de mi celular para despertarme por la mañana.
- Uso mi computadora para escuchar música en Spotify.
- Utilizo una aplicación en mi celular para cuantificar mi pasos diarios.
- Uso Whatsapp en mi celular para compartir audios con mis colegas.
- Uso Dropbox para respaldar documentos de mi computadora.

Dependiendo de la cantidad de asistentes, no es necesario que todos/as expongan su dibujo; en todo caso, se puede pedir a algunos/as que lo hagan y después que el resto complementa si tiene algún uso que no se ha mencionado.

También cuando se sabe que hay aplicaciones que sirven tanto en el celular como en una computadora o tableta, hay que indagar si se usa sólo en un dispositivo o en todos.

Al final del ejercicio, tendremos una lista de usos de la tecnología.

Actividad: ¿Qué información se produce?

Tiempo estimado: 45 minutos

Objetivo: Detallar para cada uso de la tecnología, la información que se produce. Descripción: Indicar para cada uso de la tecnología la información que se produce. Aunque parezca obvio, es necesario explicar a qué información se refiere. Por ejemplo, en el caso de una fotografía, la información que se produce no es en sí mismo el archivo digital que lo contiene, que puede ser un archivo .jpg o .png, sino lo que está en la foto; por ejemplo, qué es lo que fue tomado (un paisaje o personas), en qué momento, en qué lugar, etc. En el caso de una aplicación para taxis, la información que se produce va desde origen y destino, hasta frecuencia o forma de pago. Esta es una buena oportunidad para introducir el término **Metadatos** e incluirlo en el glosario. En este ejercicio es muy importante que se llegue al mayor detalle posible. La actividad se desarrolla completando la segunda columna de papel kraft con la información que se produce según el uso de la tecnología que se haya mencionado.

Al final del ejercicio, tendremos la lista de la información que generan la organización y sus integrantes.

Actividad: Lluvia de actores

Tiempo estimado: 30 minutos

Objetivo: Generar una extensa lista de actores que podrían tener un interés personal, político y/o económico de la información que la organización y su equipo de trabajo producen.

Descripción: La actividad consiste en discutir qué actores podrían estar interesados en cada información que se ha colocado en la lista. En esta actividad se tienen que verter todos los actores hipotéticos, sin descartar alguno, ya que en las siguientes actividades se podrán evaluar la motivación y recursos para quedarse con una lista más acotada.

Cabe explicar que la invitación es pensar en actores internacionales, nacionales, locales, políticos, grupos religiosos, periodistas, incluso en quienes pudieran tener algún tipo de interés personal, como particulares que tengan alguna inconformidad con el personal o la organización.

Durante la actividad se conecta a cada actor con la información que le podría interesar, usando plumones de colores por actor o usando estambre o hilo grueso para cada conexión. El equipo de facilitación, sin imponer puntos de vista, puede aportar información resultante de la investigación de contexto.

Tendremos una lista de actores relacionados con la información que produce la organización al finalizar el ejercicio.

Actividad: Acotando actores

Tiempo estimado: 40 minutos

Objetivo: Determinar actores que, además de tener motivación, podrían contar con los recursos necesarios para tratar de obtener información de la organización sin su consentimiento.

Descripción: Durante la actividad se discute sobre los actores mencionados: si cuentan con recursos o si se conoce que han implementando prácticas de vigilancia y/o espionaje. Se consideran recursos, no solo económicos, para poder llevar a cabo una acción: tener conocimientos, personas que pudieran ayudarles, relaciones con personas poderosas.

El equipo de facilitación debe aportar elementos sobre los diferentes tipos de recursos que se necesitan para intentar obtener información de la organización; por ejemplo: el robo de los equipos de cómputo, colocación de antenas falsas de celular, envío de malware (recordar que todos los términos nuevos se deben poner en el glosario, invitando a los participantes a escribir también).

El equipo de facilitación puede proveer de contexto sobre el marco legal y antecedentes de la vigilancia, para señalar cuáles actores están legalmente facultados para llevar a cabo la vigilancia; capacidad política o social/económica de influir sobre políticos y accesibilidad de la tecnología de vigilancia (capacidad técnica y económica).

Hay que recordar que este ejercicio tiene que ver con la percepción de cada participante, por lo que no es indispensable llegar a consensos, aunque es útil, y se puede dejar una anotación sobre las diferentes opiniones.

Con el ejercicio concluido, tendremos una lista acotada de actores que tienen capacidad de vigilancia, con interés en el trabajo de la organización.

Actividad: El semáforo de la información

Tiempo estimado: 40 minutos

Objetivo: Determinar qué información se considera sensible.

Descripción: Sobre la lista de información que la organización produce, para cada dato que pueda ser de interés para algún actor que se encuentra en la lista final de la actividad 5, se pregunta: ¿Qué harían los actores si obtienen la información? ¿Qué tan grave sería esto para la organización (sus campañas, la seguridad de sus contrapartes, la seguridad de las víctimas que acompaña, la seguridad de los integrantes de la organización, la reputación de la organización, su seguridad económica, etc.)? Si las consecuencias serían graves, poner un punto rojo. Si son consecuencias que llevan un costo importante para la organización pero son superables, un punto amarillo. Si es preferible que no ocurra pero el impacto sería mínimo o nulo, un punto verde.

Sugerencia: Insistir con los/las participantes que antes de elegir el color de semáforo justifiquen bien la elección. Por ejemplo, describiendo una situación hipotética y realista de la posible consecuencia o citando un caso parecido que haya sucedido, explicando cuál sería el impacto para la organización. Requiriendo una explicación de la propuesta de color de semáforo se fomentan la discusión y el debate entre los participantes, ayuda a que los resultados finales del diagnóstico estén realmente consensuados.

Al concluir la actividad, tendremos una lista de la información que se tiene que proteger de la vigilancia: todos los datos que tienen puntos rojos o amarillos.

Actividad: Puertas y candados para la información

Tiempo estimado: 15 minutos



(/wiki/index.php/File:16_ManualSD_TR.png)

Objetivo: Describir los mecanismos de protección que existen sobre la información sensible de la organización.

Descripción: Para toda la información que tiene que protegerse de la vigilancia, teniendo a la lista de “usos de tecnología” como referencia, preguntar dónde se encuentra esta información y cuáles medidas se han tomado hasta ahora para resguardarla y/o limitar el acceso de terceros a ella (llave, cifrado, contraseña, ubicación, temporalidad, nada, **respaldos**, etc.). Apuntar las respuestas.

En esta actividad es necesario tratar de recuperar los saberes intuitivos que los miembros de la organización usan. Algunos no tendrán base alguna y puede ser un momento adecuado para eliminar falsos supuestos, pero en otros es posible sorprendernos con las estrategias que la gente desarrolla.

Al terminar el ejercicio, tendremos una lista de los usos de la tecnología por parte de la organización y sus integrantes, los cuales requieren la incorporación de mejores prácticas y herramientas de seguridad digital.

Comentarios de cierre del trabajo colectivo

Tiempo estimado: 15 minutos

Para poder concluir la sesión grupal se pregunta a los/as asistentes si en su percepción han tenido incidentes de seguridad en general y digital, en particular. Después, si se siente ansiedad o malestar en el grupo, hay que tratar de generar un diálogo sobre la importancia del diagnóstico como primer paso, proceso que nunca será perfecto sino que estará en transformación constante pero que será útil. Se puede recurrir a alguna dinámica corporal que ayude con el estrés.



(/wiki/index.php/File:22_ManualSD_TR.png)

Para cerrar, se explica que el siguiente paso es la revisión del ambiente físico y de los equipos de cómputo, enfatizando que no se trata de un análisis forense y que tampoco será el momento de instalar programas o arreglar problemas que se presentan, sino una mirada **a vuelo de pájaro** de estructura de la información que se guarda, programas, estado de antivirus. Hay que reforzar que no será un análisis que violente la privacidad, puesto que para algunas personas mostrar sus equipos de cómputo puede ser como mostrar el clóset de su habitación o el cajón que está al lado de la cama. También se aprovecha para recordar la importancia de contar con la total asistencia de quienes participarán en la sesión de retroalimentación de los hallazgos preliminares.



(/wiki/index.php/File:23_ManualSD_TR.png)

Probablemente, un análisis más exhaustivo incluiría la revisión de móviles pero, a partir del análisis de las computadoras y de la actividad sobre usos de la tecnología, se pueden inferir muchas de las vulnerabilidades. Lo que se busca es no exponer a las personas en su intimidad. Concluyendo la sesión hay que recordar que la información deberá guardarse en un lugar seguro.

Nota: Dependiendo del tiempo, se recomienda tomar uno o dos descansos.

Análisis del ambiente físico y de los equipos de cómputo

La seguridad digital depende también de las condiciones ambientales en las que se usan los dispositivos. Por tanto, es pertinente realizar una evaluación sistemática de algunos aspectos específicos de las instalaciones de trabajo, incluyendo:



(/wiki/index.php/File:17_ManualSD_TR.png)

a) La facilidad para acceder a la oficina: cuántas puertas y ventanas tiene y si están bien protegidas, si es fácil acceder desde alguna construcción vecina, etc.

b) Si la oficina cuenta con portero y si se cumple el protocolo acordado con él para el ingreso.

c) La existencia de alarmas y cámaras de seguridad. En caso de contar con cámaras, hay que asegurarse que funcionan y si graban. En ese caso, preguntar la existencia de protocolos para revisar los videos. También si tienen una pila para la alarma, en caso de un corte de energía eléctrica.

d) Si en la oficina hay espacios que se cierran bajo llave, conocer quiénes tienen las llaves y acceso a qué espacio. Si hay archiveros, también saber quiénes.

e) Otro aspecto a evaluar es si se recibe a gente externa a la organización en una sala en particular, y si los/as visitantes podrían desde ahí dirigirse fácilmente a otra área dentro de la oficina (se busca saber si es posible robar equipos o dejar un dispositivo tipo keylogger).

f) Estado de la construcción, especialmente si hay humedad, y si las conexiones eléctricas están en buen estado. También verificar si hay sobrecarga de dispositivos en una misma conexión y si se usan reguladores.

Como parte de esta revisión general hay que observar si las computadoras están conectadas usando una red inalámbrica o por ethernet, la configuración de la red, la fortaleza de la contraseña de la red inalámbrica, si el módem ha cambiado su configuración de origen y la compañía que ofrece el servicio.

Para la revisión de los equipos de cómputo hay que recordar que no se trata de un análisis forense y la profundidad con la que se realice depende de los conocimientos técnicos del equipo de facilitadores y el tiempo. En caso de sospechar la presencia de **malware**, si se quiere documentar para tomar acciones legales, es mejor no trabajar sobre el equipo y generar una copia. Por sí mismo, esto es un trabajo independiente, pero si se requiere se puede iniciar con un sistema en vivo GNU-Linux (el comando dd puede ser una opción).

Considerando el tiempo promedio que requiere el análisis de las computadoras, recomendamos intentar hacer al menos 10 equipos que correspondan a las diferentes áreas de trabajo, ya que lo que se pretende es tener una muestra lo más completa posible.

El análisis de las computadoras se concentra en tres puntos: a) vulnerabilidades en los equipos por ausencia de antivirus, desactivación de firewall o falta de actualizaciones de seguridad; b) instalación y uso de programas que tienen vulnerabilidades, malware, adware u otro tipo de software malicioso; c) exposición por uso del navegador de internet.

Para poder evaluar los puntos anteriores, en el caso del sistema operativo Windows, desde la terminal cmd se pueden usar los siguientes comandos: systeminfo, tasklist y wmic. Después se va al visor de eventos y se guardan los logs de eventos de seguridad, de hardware, aplicación, administrativos, instalación y sistema para una revisión rápida.

En OS X puedes usar Información del sistema y la consola para mirar los logs. En GNU-Linux hay una variedad amplia de comandos para listar programas y ver los logs.

Se revisa el estado de firewall.

Se detecta si se tiene antivirus, versión de la base de datos y logs. Si no se tiene antivirus o está desactivado se debe considerar usar una de las versiones en vivo.

Se revisa que navegador/es se usan, guardado del historial, guardado de contraseñas y plugins instalados.

Sugerencia: dependiendo de las habilidades del equipo de facilitación, se puede generar un script para automatizar la revisión del firewall y de los logs.

Sugerencia: Al revisar los logs también es posible automatizarlos mediante un script, es importante poner atención en las direcciones IP recurrentes.

Sugerencia: Puedes hacer un mapeo completo de la red para verificar equipos conectados y usuarios. Para la Wifi puedes verificar tipo de cifrado, vpn y/o vlan.

Evaluación del día y revisión de archivos

Para lograr concluir el trabajo en tiempo, el tener una breve reunión de evaluación en la que se puedan intercambiar observaciones,



(/wiki/index.php/File:18_ManualSD_TR.png)

posibilidades para el segundo día, preocupaciones, aspectos positivos del trabajo y cómo se siente el equipo de facilitación, hará más eficiente el tiempo restante.

A partir de la reunión general y los primeros resultados de los equipos de cómputo, se puede iniciar ya la sistematización para la redacción del informe preliminar. En el anexo 1 podrás encontrar una propuesta de formato. El objetivo en general es organizar la información, considerando los riesgos encontrados y, a partir de ello, proponer una ruta de fortalecimiento en seguridad digital para la organización.

El informe debe considerar:

- Hallazgos de la evaluación del ambiente físico.
- Análisis de amenazas a la información:

a) Riesgo: Pérdida de información por fallo de hardware, robo o pérdida de hardware, o error humano

b) Riesgo: Pérdida de información por ataque de malware y

c) Riesgo: Vigilancia o robo de datos.

- Recomendaciones.

Para este momento se tendrá además mucha información que revisar y procesar. Sobre los archivos que se tienen de los equipos, hay que evaluar programas instalados y, si hay algunos que son poco comunes, investigar sobre ellos. **En otros casos se conocen más las vulnerabilidades**, por ejemplo: en programas para comunicación por voz si usan o no cifrado en tránsito. Para los logs, lo que se necesita es una vista **a vuelo de pájaro**, entonces se tiene que relacionar la información con lo que la gente ha manifestado que hace o detectar si se reportó algún incidente extraño. Por ejemplo, si el trabajo en la oficina es siempre matutino, será anormal encontrar que hay un reporte de inicio del sistema por la noche. También hay que familiarizarse con los procesos que comúnmente se ejecutan en los diferentes sistemas operativos para observar si hay procesos inusuales.

La profundidad con la que se logre la revisión de eventos del sistema y lista de tareas, depende mucho de los conocimientos y la experiencia que tiene el equipo de facilitación. Para introducirse en el tema es útil investigar aspectos como los programas comunes de inicio de los sistemas operativos y los códigos de errores. La idea muchas veces no es encontrar un error sino buscar patrones y anomalías.

Día 2



(/wiki/index.php/File:13_ManualSD_TR.png)

La jornada del segundo día consiste en tres etapas: 1) Primera conclusión de la revisión de los equipos de cómputo; 2) la redacción del informe preliminar; y 3) la discusión del mismo con la organización.

Conclusión del análisis de equipos de cómputo y redacción del informe preliminar

Lo deseable es ocupar entre tres y cuatro horas para terminar con la revisión de los equipos para dejar suficiente tiempo para concluir el informe preliminar (aproximadamente dos horas) y reservar unos minutos para la impresión.

En la redacción del informe hay que tener cuidado con proveer una argumentación sólida que justifique las recomendaciones. Si bien el objetivo no es redactar una explicación extensa sobre cada vulnerabilidad encontrada, en algunos casos ayudará para apropiarse de la propuesta, entender el por qué algo es considerado un riesgo. El informe debe poder hilar aspectos de contexto social, político y económico con aspectos más técnicos. También, sin minimizar los riesgos, se debe ser responsable con la forma en la que se plantean las vulnerabilidades.

Las recomendaciones deben asumir las condiciones reales de cada organización. A veces la mejor opción es la que, en efecto, se podrá implementar; de nada sirve proponer cambiar de equipos o poner un servidor interno si no hay condiciones. Sin embargo, es posible sugerir recomendaciones a largo plazo. Las propuestas deben ser claras respecto a los requerimientos para ser implementadas, incluyendo los tiempos. En nuestra experiencia, es importante poder comprometer a la organización en acciones a corto plazo que alienten su interés y visibilicen que es posible tomar algunas acciones. De tal forma, la seguridad como un paso a la vez, se fortalece con prácticas más autónomas.

En el Anexo I se encontrará se sugiere una plantilla para que facilitar el proceso de redacción del reporte preliminar.

Presentación del informe preliminar



(/wiki/index.php/File:20_ManualSD_TR.png)

El tiempo estimado para esta actividad es de dos horas. Se inicia explicando que el informe es una primera versión que tiene como objetivo compartir con la organización los hallazgos y las recomendaciones, que es un momento valioso para hacer cambios por si se ha entendido mal alguna cosa o si hay información que no quedó incluida, y que se alcance un acuerdo interno con el equipo de facilitación respecto a las recomendaciones finales.

Se dan unos minutos para que cada participante lea el informe y, posteriormente, se hace una lectura colectiva, dando la oportunidad para la retroalimentación.

En la sección de recomendaciones es fundamental que quede claro lo que se propone, tiempos, y las razones por las cuales se hace cada recomendación.

Finalmente, se crea un acuerdo sobre el medio oportuno para hacer la entrega del informe final y la confidencialidad de la información, acordar como se destruye el papel kraft usado y si es necesario destruir también las copias del informe preliminar. Si aún queda algo de tiempo se puede pedir una breve evaluación de los/as participantes sobre la experiencia del diagnóstico en el ánimo de hacerlo cada vez mejor.

En el caso de que el equipo facilitador tenga que conservar algunos archivos del análisis de computadoras para un análisis más profundo, debe considerar la vía más segura para transportarlos, guardarlos y borrarlos posteriormente.

Diagnóstico final



(/wiki/index.php/File:19_ManualSD_TR.png)

La versión final del informe del diagnóstico debe incluir todos los cambios sugeridos en la reunión de retroalimentación. Su elaboración es una oportunidad para añadir una argumentación más detallada sobre vulnerabilidades,

empresas, condiciones económicas y/o políticas. Inevitablemente implicaría investigación adicional para poder llenar huecos de información que no se pudieron resolver durante la actividad de análisis de amenazas, y para contar con la información más actualizada sobre las herramientas cuyas ventajas y desventajas se evaluaron. La investigación es fundamental para maximizar la pertinencia de las recomendaciones y la claridad de su justificación.

El último paso en el diagnóstico es hacer llegar el reporte final a la organización. Es importante que se envíe por un medio seguro, ya que el reporte puede contener información altamente sensible sobre la organización, y también para establecer un buen antecedente al manejar cuidadosamente el transporte de información sensible.



(/wiki/index.php/File:21_ManualSD_TR.png)

Recursos útiles

Sin duda, mantenerse actualizado sobre las herramientas y tener acceso a información que nos ayude en los procesos formativos de seguridad digital, es complicado. A continuación, listamos algunos recursos útiles, pero hay que recordar que los cambios en el tema se están dando en tiempos muy cortos, por lo que hay que buscar actualizarse y, si se tiene la oportunidad, compartir los recursos que se encuentren con la comunidad.

- Manual Zen (https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual/es)
- Seguridad en una caja (<https://securityinbox.org/es/>)
- Autoprotección Digital Contra La Vigilancia: Consejos, Herramientas y Guías Para Tener Comunicaciones Más Seguras (<https://ssd.eff.org/es>)
- Documentos de Fundación Karisma (<https://karisma.org.co/biblioteca/>)
- Guía de Seguridad Digital para Feministas Autogestivas (<https://es.hackblossom.org/cybersecurity/>)

En inglés:

- Seguridad holística (<https://holistic-security.tacticaltech.org>)
- SAFETAG (<https://safetag.org/>)
- Level-up (<https://level-up.cc/>)

Agradecimientos

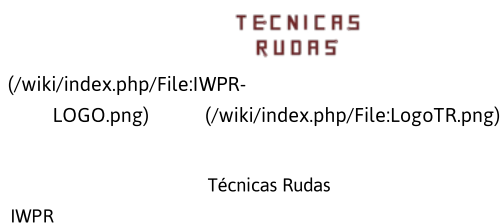


(/wiki/index.php/File:25_ManualSD_TR.png)

Agradecemos profundamente a Jacobo Nájera, Hedme Sierra Castro y William Vides por su revisión de la versión en español y a Alexandra Hache por la lectura de la primera versión de este documento. Agradecemos también a Mónica Ortiz por la corrección ortográfica y de estilo.

Créditos

Esta guía fue escrita por Técnicas Rudas (<http://tecnicasrudas.org>) con el apoyo del "Institute for War and Peace Reporting" IWPR (<http://iwpr.net>).



Diseño: María Silva y Yutsil Mangas

Anexo I

Plantilla para el reporte final del Diagnóstico en Seguridad Digital
(https://gendersec.tacticaltech.org/wiki/images/8/8c/Diagn%C3%B3sticoSeguridadDigital_InformePreliminar_Plantilla.odt)

Versión en inglés

Versión al inglés
(https://gendersec.tacticaltech.org/wiki/index.php/Digital_Security_Assessment_for_Human_Rights_Organizations:_A_guide)

Referencias

1. <https://r3d.mx/2017/06/19/gobierno-espia/> (<https://r3d.mx/2017/06/19/gobierno-espia/>)
2. <https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf>
(<https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf>)
3. https://en.wikipedia.org/wiki/Global_surveillance_disclosures_%282013%E2%80%93present%29
(https://en.wikipedia.org/wiki/Global_surveillance_disclosures_%282013%E2%80%93present%29)
4. Sobrepasa los alcances de este manual detallar aspectos de la educación popular y existe numerosa bibliografía al respecto. Se puede iniciar revisando la obra de Paulo Freire (Por ejemplo: https://es.wikipedia.org/wiki/Paulo_Freire (https://es.wikipedia.org/wiki/Paulo_Freire))
5. El término popularmente se refiere a una actitud obsesiva que se refleja en la búsqueda de información pero que puede llegar más lejos.
6. IPI Información Personal Identificable se refiere a toda aquella información sobre un individuo que es administrada por un tercero (por ejemplo: gobiernos o empresas), incluyendo todos aquellos datos que pueden ser distintivos del individuo o a partir de los cuales es posible rastrear su identidad y toda la información asociada o asociable al individuo (por ejemplo: el número de su pasaporte, su dirección física, la placa de matriculación de su coche, etc).
7. Un sistema operativo en vivo (o Live en inglés), es un sistema que puede iniciarse sin necesidad de ser instalado en el disco duro de la computadora, comúnmente a partir de un disco o un dispositivo de almacenamiento externo (USB) o por medio de la red, usando imágenes para netboot. Los sistemas Live no alteran el sistema operativo local o sus archivos, en algunos casos puede seguirse un procedimiento para que sean instalados en el disco duro de la computadora.

Disponível em "[https://gendersec.tacticaltech.org/wiki/index.php?](https://gendersec.tacticaltech.org/wiki/index.php?title=Diagnósticos_en_seguridad_digital_para_organizaciones_defensoras_de_derechos_humanos_y_del_territorio:_un_manual_para_facilitador)

[title=Diagnósticos_en_seguridad_digital_para_organizaciones_defensoras_de_derechos_humanos_y_del_territorio:_un_manual_para_facilitador](https://gendersec.tacticaltech.org/wiki/index.php?title=Diagnósticos_en_seguridad_digital_para_organizaciones_defensoras_de_derechos_humanos_y_del_territorio:_un_manual_para_facilitador)
([https://gendersec.tacticaltech.org/wiki/index.php?](https://gendersec.tacticaltech.org/wiki/index.php?title=Diagnósticos_en_seguridad_digital_para_organizaciones_defensoras_de_derechos_humanos_y_del_territorio:_un_manual_para_facilitador)

[title=Diagnósticos_en_seguridad_digital_para_organizaciones_defensoras_de_derechos_humanos_y_del_territorio:_un_manual_para_facilitador](https://gendersec.tacticaltech.org/wiki/index.php?title=Diagnósticos_en_seguridad_digital_para_organizaciones_defensoras_de_derechos_humanos_y_del_territorio:_un_manual_para_facilitador)

Categorías (/wiki/index.php/Special:Categories): [How To](#) (/wiki/index.php/Category:How_To)

[Resources](#) (/wiki/index.php?title=Category:Resources&action=edit&redlink=1)