CIBERMUJERES

Introducción

Introducción

https://iwpr.net/

Índice general

Introducción a Cibermujeres

A lo largo de los últimos años, han surgido numerosos esfuerzos para crear recursos, metodologías y prácticas mejoradas para capacitaciones en seguridad digital; sin embargo, pocos resultados han incorporado una perspectiva de género de manera consolidada y consistente. Más recientemente, gracias a los esfuerzos dentro de los movimientos de mujeres y feministas en todo el mundo, ha empezado a emerger un abanico de contenidos sobre seguridad digital enfocadas en temas de género. Aún así, persiste la falta de coordinación en la comunidad de seguridad digital para alimentar esta colección de recursos de una manera estratégica y respondiendo a los contextos.

Con este fin, IWPR ha construido la currícula Cibermujeres con la intención de resonar las técnicas y prácticas desarrolladas por defensoras de derechos humanos (WHRDs) que lideran iniciativas de capacitación en seguridad digital en la región de Latinoamérica y el Caribe (LAC). Basándonos en la experiencia del trabajo de estas mujeres, hemos creado, desde un abordaje coconstruido y desde una perspectiva de género, este contenido original para formadoras en seguridad digital que trabajan con defensoras de las libertades y derechos.

Para evitar duplicar esfuerzos, identificamos materiales ya existentes que respondieron a las necesidades y contextos de las defensoras: por ejemplo,

algunos contenidos de la currícula de LevelUp o recursos desarrollados por organizaciones como Tactical Technology Collective (TTC) y Association for Progressive Communications (APC). Dichos contenidos han sido incorporados directamente en la currícula, con su respectiva atribución y créditos. Sin embargo, el valor y aporte esencial de este material reside en los módulos y las recomendaciones creadas específicamente para esta currícula con el fin de brindar experiencias de aprendizaje hechas a medida para los contextos de las defensoras que trabajan en entornos de alto riesgo.

Cómo utilizar la Currícula de Cibermujeres

Esta currícula ha sido diseñada tomando en cuenta dos tipos de perfiles: por un lado, formadoras que buscan conducir capacitaciones sobre seguridad digital con perspectiva de género a grupos de mujeres; por otro lado, mujeres que han recibido una capacitación y quieren transmitir este conocimiento sobre seguridad digital a sus redes de compañeras/os y activistas. El conjunto completo de sesiones no es relevante para todos los públicos, así que te animamos a identificar y enfocar las que cobran valor y sentido para la comunidad con la que trabajas.

Cibermujeres incluye juegos interactivos, materiales gráficos y audiovisuales, además de guías para apoyar a las facilitadoras. Los módulos pueden utilizarse por separado o combinados para diseñar un taller completo. Esta estructura modular permite a las formadoras seleccionar contenidos específicos que se ajustan a las necesidades de las participantes de la capacitación o, si así prefieren, también pueden seguir las secuencias (rutas) de módulos sugeridas. Si quisieras cubrir toda la currícula de principio a fin, necesitarías aproximadamente 10 días completos; para quienes quieran facilitar una capacitación de este tipo, recomendamos espaciar las sesiones a lo largo de seis meses. Con este abordaje, las participantes tendrán suficiente tiempo para integrar, de manera eficaz, nuevas técnicas y herramientas en sus prácticas personales de seguridad digital antes de avanzar a desarrollar nuevas habilidades.

Además, como parte de este enfoque en seguridad holística, la currícula

incorpora contenidos específicos sobre auto-cuidado feminista y reconoce la violencia de género, tanto simbólica como online. El objetivo de estas sesiones es reforzar el sentido de apropiación y control de las participantes sobre su seguridad e identidades. Por lo tanto, es importante que sean integrados estos temas transversales a lo largo de las capacitaciones como oportunidades para la acción y reflexión colectiva e individual, y no como módulos aislados.

Hay muchas actividades y ejercicios incluidos en esta currícula: algunas son para fortalecer la confianza –recomendamos empezar por aquí, al principio de todo–; otras sirven para romper el hielo al arrancar cada día del taller. Finalmente, algunas actividades están diseñadas para fortalecer ciertos contenidos de capacitación y tienen un orden determinado. La currícula también incluye materiales complementarios para dar seguimiento a lo largo de los seis meses de duración sugerida.

Una perspectiva feminista en la creación de esta currícula

Como comentamos anteriormente, esta currícula integra una visión holística sobre la seguridad para defensoras de derechos humanos, incluyendo la "tríada" seguridad digital, seguridad física y auto-cuidado. Cabe mencionar que nos enfocamos en el componente de seguridad digital. Para un abordaje más transversal y sensible a temas de género y más feminista, esta currícula fue producida con los siguientes valores y principios medulares en mente – animamos enfáticamente que las formadoras y facilitadores las tomen en cuenta cuando diseñen sus talleres utilizando esta currícula:

Mujeres participantes y mujeres formadoras

Primero, y sobre todo, los contenidos de Cibermujeres están diseñados para apoyar la confianza y autoestima entre mujeres en el contexto del taller. Las participantes suelen venir de entornos –tanto física como emocionalmente– de alto estrés y ansiedad; las defensoras de derechos humanos suelen ser el blanco de acoso y violencia online y offline. Es esencial que perciban la

capacitación como un espacio seguro donde puedan sentirse cómodas compartiendo sus miedos, dudas y emociones, y que puedan participar e interactuar entre ellas activamente. Por lo tanto, esta currícula está dirigida a mujeres formadoras trabajando con participantes mujeres. Sin embargo, también alentamos que formadores hombres y diversos revisen esta currícula y sus principios fundacionales para adaptar mejor su praxis en talleres con grupos mixtos.

Modelos femeninos y feministas

Esta currícula ha sido creada con un enfoque específico en el intercambio de experiencias personales de ataques digitales –tal cual han sido vividas por las defensoras, activistas y periodistas– a través de testimonios que empoderen. Reconociendo que no todas las mujeres en el taller van a definirse como feministas, el abordaje que proponemos del proceso de capacitación se centra en crear conciencia sobre la violencia en línea contra las defensoras; primero subrayando las diferencias entre los ataques dirigidos hacia hombres y mujeres activistas; después, proporcionando ejemplos de violencia de género en línea (ej. en plataformas de redes sociales) como una manera de ayudar a las mujeres a identificar la violencia que quizás ya hayan afrontado en estos espacios.

Como parte de esta metodología, presentamos estudios de casos cercanos al día a día de las mujeres, facilitando que las participantes puedan relacionarse a diferentes situaciones y comprender la relevancia que cobran en sus propios contextos. Nos dimos cuenta que este abordaje empodera a las mujeres y las anima a practicar, de manera más consistente, nuevas habilidades y transmitir a otras personas consejos sobre seguridad digital.

¡Mi cuerpo, mis dispositivos, mi decisión!

Las principales ideas, información y prácticas compartidas en esta currícula se arraigan en promover la autonomía digital. El énfasis del "pensamiento estratégico sobre la seguridad digital" es el núcleo del diseño de esta guía:

compartir conceptos de seguridad digital con las participantes en vez de entrenarlas en una lista de herramientas. Invertimos una gran parte del tiempo a presentar conceptos de seguridad digital como el cifrado, el anonimato, la privacidad y el software open-source, antes de capacitar en las herramientas relacionadas. Apoyar a las mujeres a desarrollar su propia comprensión de estos conceptos ayuda a que se lleven la información necesaria para tomar sus propias decisiones sobre qué herramientas son mejores para ellas.

Análisis de riesgos con perspectiva de género de género en plataformas de redes sociales

Utilizamos ejemplos de vídeos de Youtube, mensajes en diferentes plataformas de redes sociales y resultados de otras sesiones de capacitación con el objetivo de crear un espacio seguro para la discusión y reflexión sobre violencia de género que surge en una dimensión de tecnologías digitales. Específicamente, la gran parte de lo mencionado converge en el módulo de "Violencia en línea contra mujeres"; de igual manera, el ejercicio "Modelo de riesgos con perspectiva de género" incluido en el módulo "Buscando la mejor solución" se centra en compartir experiencias e identificar las vulnerabilidades que las participantes enfrentan, no sólo por ser mujeres, sino por realizar actividades críticas a los roles hegemónicos: activismos, comunicación, organización, creación...

Auto-cuidado feminista & Defensa personal digital

Como parte de un abordaje holístico de la seguridad, esta currícula contempla el bienestar emocional y el auto-cuidado como elementos vitales de la seguridad para las defensoras; en este mismo sentido, como parte del enfoque de la autonomía digital, hay sesiones específicas –como la sesión "Modelo de riesgos con perspectiva de género"– que tienen la intención de ayudar a las participantes a prepararse para y reaccionar ante ataques digitales. Esta guía es un esfuerzo para brindar información a las participantes para que identifiquen y exploren diversas estrategias para su defensa personal digital;

éstas incluyen, pero no se reducen a: separar la esfera personal de la pública, crear identidades online, "hacer doxxing al troll", cifrar comunicaciones y documentar incidentes digitales. Preparar a las participantes con una mejor comprensión sobre su entorno online —en las plataformas que utilizan y los riesgos asociados a ellas— nos permite empoderarlas en desarrollar hábitos robustos de seguridad digital que puedan formar parte de una práctica holística de auto-cuidado.

Planeando recursos

- **Objetivos:** Diagnóstico y evaluación antes de empezar la capacitación
- **Formato:** Anexo

Diagnóstico y evaluación antes de empezar la capacitación

Realizar un diagnóstico antes de diseñar la capacitación es crucial. Obtener una comprensión profunda sobre las necesidades en seguridad digital de las participantes ayuda a asegurar una capacitación efectiva y una experiencia de aprendizaje adaptada a sus contextos y objetivos. Conocer la experiencia que tienen las participantes con las tecnologías -cómo las utilizan y se comunican con ellas- tiene un impacto significativo en el espectro de contenidos que vamos a cubrir en nuestro taller.

Evaluando necesidades y motivaciones

Idealmente, las formadoras llevarán a cabo una evaluación de necesidades antes de la capacitación, trabajando con las participantes o con una representante de su organización o colectivo. Toma en cuenta que, más allá de

objetivamente evaluar sus necesidades, será importante también comprender sus motivaciones en participar en la capacitación: ¿están proactivamente buscando fortalecer su propia resiliencia o están solicitando apoyo en respuesta a incidentes recientes o aún en curso? Además, en un sentido más pragmático, contempla que la cantidad de contenidos en las sesiones tiene que concordar con el objetivo de las personas o el grupo y con las habilidades de las mismas. El conjunto de saberes colectivos de las participantes también será un factor determinante.

Si tienes la oportunidad de interactuar y comunicarte con las participantes en más profundidad antes del taller, aquí sugerimos una serie de preguntas que puedes plantear para aprender más sobre ellas y/o el grupo con el que trabajan:

- ¿Cuál es la trayectoria del grupo?
- ¿Cómo está configurado el grupo? ¿Cómo se organiza?
- ¿Cuáles son sus objetivos, agendas y actividades?
- ¿Cuáles son algunas de sus prácticas relacionadas con las tecnologías? ¿Cómo y desde dónde acceden a Internet?
- ¿Qué tipo(s) de computadoras y/o dispositivos móviles utilizan? ¿Usan dispositivos separados para su actividad personal y profesional?
- ¿Qué sistemas operativos utilizan?
- ¿Con qué movimientos y/o grupos colaboran? Puede ser como representante de su organización (ej. como miembros de una coalición o red) o a nivel personal como activistas independientes.
- ¿Han experimentado incidentes o amenazas directas hacia su seguridad física y/o digital? Ello puede estar relacionado con sus dispositivos, infraestructura y posesiones, cuentas online y/o agresiones físicas.

Herramienta de seguridad digital y capacidades (DISC)

Si tienes la oportunidad de entablar un proceso de evaluación y diagnóstico integral con las participantes antes del taller, la herramienta DISC incluida en esta currícula puede ser útil para ti. Es un recurso creado por IWPR y es utilizado ampliamente en procesos de diagnóstico y evaluación pre-capacitación.

La herramienta DISC es un cuestionario que utiliza un mecanismo de puntuación cuantitativa para medir el nivel de conocimientos y habilidades que tienen las participantes en temas de seguridad digital. También brinda información cualitativa sobre las fortalezas y ámbitos que pueden mejorarse a un nivel más detallado y enfocado en las praxis. Si vas a estar trabajando de manera constante con las participantes (por ej, sesiones durante 6 meses), la herramienta DISC puede ser útil para monitorear avances de aprendizaje y comprensión.

La herramienta DISC completa puede encontrarse aquí[1]

Estrategias alternativas de evaluación y diagnóstico

Si no puedes realizar directamente un diagnóstico antes de la capacitación, ni obtener respuestas a estas preguntas comentadas anteriormente, todavía puedes conseguir bastante información sobre las trayectorias de las participantes a partir de sus contextos y circunstancias:

Por ejemplo, si conoces a mujeres y organizaciones activistas que están haciendo un trabajo parecido en la misma región que los grupos con los que vas a trabajar, es probable que hayan enfrentado riesgos y/o ataques similares.

Además, posiblemente haya amenazas o incidentes que correlacionan con el tipo de trabajo que las participantes realizan (y los lugares donde actúan). Si vas a estar capacitando abogadas que acompañan a otras defensoras

[1] https://cyber-women.com/es/DISC/

o periodistas que denuncian casos de corrupción gubernamental, puedes investigar las tácticas que actores estatales y no estatales han aplicado contra individuos, particularmente hacia mujeres, que operan en el mismo país y en ámbitos parecidos.

Ejemplos de rutas de capacitación

Aunque nos damos cuenta que el contenido final de la capacitación se basará en el diagnóstico que cada formadora realice sobre el grupo con el que va a trabajar, compartimos varias rutas a modo de ejemplo.

Las rutas a continuación se organizan por duración (en días) y por nivel de habilidades. Otros parámetros entran en juego a la hora de planear la capacitación, pero generalmente el factor tiempo es el más crítico:

El tiempo del que dispones determina, en última instancia, cuánto contenido puedes cubrir en un taller; el conjunto de saberes de las participantes también será un factor determinante.

Es más probable que sepas de antemano de cuánto tiempo dispones antes de saber otros factores como el espacio donde se va a realizar el taller, el número de participantes o su nivel de conocimientos/experiencias.

Leer más[2]

[2] https://cyber-women.com/es/rutas/

Agradecimientos

Algunas sesiones y contenidos adaptados para la currícula fueron desarrollados originalmente por: Association for Progressive Communications, Tactical Technology Collective, Fundación Karisma, Mujeres Al Borde, Elis Monroy de Subversiones Collective, Danah Boyd, Mariel García, Alix Dunn, Spyros Monastiriotis y Phi Requiem y mantienen la licencia publicada por sus autores. Los contenidos desarrollados en especial para esta página tienen una licencia Creative Commons - Atribución, Compartir Igual.

- **Autoras:** El contenido original de esta currícula fue desarrollado por Alma Ugarte Pérez, Hedme Sierra Castro e Indira Cornelio Vidal
- **Coordinación:** Dhaniella Falk y Alejandra Garcia y Dainna James
- **Educación y Localización:** Nicholas Sera-Leyva, Azza Sultan, Mohammed Al-Maskati y Ali Sibai
- **Traducción al español:** Nadège Lucas Pérez
- **Coordinación del Aprendizaje entre Pares y Piloteo de las Sesiones:** Estrella Soria
- **Consultoría:** Cooperativa Tierra Común[1]
- **Desarrollo web, diseño gráfico y producción audiovisual:** Cooperativa

[1] https://tierracomun.org

Kéfir[2]

- **Revisión entre pares y colaboradoras:** Azza Sultan, Carol Waters, Dalia Othman de Tactical Technology Collective, Estrella Soria, Erika Smith de la Association for Progressive Communications, Gigi Alford, Jennifer Schulte, Laura Cunningham, Lindsey Andersen, Megan DeBlois de Internews y Sandra Ordoñez.

[2] https://kefir.red/

Política de Uso de Datos de CiberMujeres

Última actualización: 4 de Septiembre de 2018. Documento producido por Kéfir

Contexto

Antes de entrar en detalles concretos sobre cómo utilizamos los datos generados en esta plataforma y qué puede hacer para ser agente de este proceso, vamos a introducir un contexto general.

Sobre el proyecto

La currícula de CiberMujeres fue creada e implementada por IWPR como parte del proyecto "Seguridad, Concientización y Acción" (Safety, Awareness and Action -SAWA-) y financiada por la Oficina de Democracia, Derechos Humanos y Trabajo ("Bureau of Democracy, Human Rights and Labor -DRL-") del

Departamento del Estado de EEUU.

La plataforma web está diseñada y desarrollada por Kéfir[1]. También se encargaron del diseño frontend y el diseño gráfico. Kéfir, hasta la actualidad, administra el servidor donde está alojada la plataforma.

Puedes leer más sobre el proyecto de CiberMujeres aquí[2].

El Derecho a la Privacidad

El Derecho a la Privacidad se define como un derecho humano, explícitamente enunciado en el Artículo 12 de la Declaración Universal de Derechos Humanos de 1948.

"Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."

Regulaciones

Aparte del marco de derechos humanos, existen regulaciones específicas en torno a los datos. ¿Quizás te suene familiar las siglas GPDR?

El "Reglamento General de Protección de Datos"[3] (en inglés "General Data Protection Regulation") entró en rigor a partir del 25 de Mayo de 2018.

Esta regulación europea está diseñada para proteger mejor a las personas de brechas de seguridad e incumplimientos contra la privacidad. La nueva ley, entre otros aspectos, estipula cómo las empresas deben manejar los datos de sus clientes.

[1] https://kefir.red/

[2] https://cyber-women.com/en/#about

[3] https://es.wikipedia.org/wiki/Reglamento_General_de_Protecci%C3%B3n_de_Datos

Desafortunadamente, estas regulaciones no se aplican en todos los contextos y tampoco son suficientes en si mismas. Ciertas jurisdicciones albergan una comprensión y abarcan la privacidad de una manera relativamente buena; otras se quedan bastante atrás.

Existen personas y grupos que, desde el ámbito de la promoción de políticas públicas están luchando por una equidad al acceso a la privacidad.

Les invitamos a leer el comunicado de la Asociación para el Progreso de las Comunicaciones Progresistas sobre el PGPD[4].

Cumplimiento

Todos los sitios y plataformas visitadas por personas ciudadanas de jurisdicciones que regulan la privacidad de datos deben proporcionar acceso a un documento legal obligatorio que explica cómo recolectan, almacenan, procesan y comparten información de identificación personal.

Información de identificación personal (en inglés "Personal Identifiable Information -PII-): cualquier información relacionada con una persona identificada o identificable ('persona afectada o interesada'/'sujeto de datos'); una persona identificable es aquella que puede ser identificada, directa o indirectamente. Ejemplos de estos datos personales incluyen, pero no se limitan a: nombre, número de seguridad social, cédula de conducir, otros identificadores del Estado; ciudadanía, estátus legal, género, origen étnico/racial, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, datos genéticos y biométricos (que pueden identificar a una persona concreta si son procesados); datos de contacto de emergencia, etc.

Recolectar y usar datos no genera daños necesariamente. Los datos se pueden utilizar para cumplimientos legales o relacionados con rendir cuentas a financiadoras, además de obtener retroalimentación y mejorar herramientas. Lo importante es la transparencia en cómo estos datos son recolectados, almacenados, procesados y compartidos.

[4] https://www.apc.org/fr/node/34716

El compromiso de CiberMujeres hacia la privacidad

Más allá de cumplir con ciertos mínimos, esta plataforma ha sido diseñada y desarrollada por activistas que buscan integrar la privacidad como un valor, posicionamiento y práctica ética.

No sólo evitamos identificar individuos sino que nos desmarcamos de generar datos que puedan ser utilizados fuera de los intereses de las personas navegantes de esta plataforma.

Generalmente, las políticas de datos son abstractas, perdidas en letra pequeña y bastante crípticas. Esta tendencia refleja una falta de transparencia y responsabilidad social, muchas veces con la intención de ocultar un modelo de negocios y colaboraciones con terceros que no serían de agrado para vosotras.

En Ciber Mujeres, nuestra Política de Uso de Datos es una extensión de este proyecto: una oportunidad para aprender sobre nuestro derecho a la privacidad, cómo puede tomarse en cuenta y cómo llevarla a la práctica.

Qué estamos haciendo

Cookies y código de terceros

Cuando visitas un sitio web, sus contenidos se cargan desde diferentes fuentes (dominios y servidores). Este funcionamiento es lo que caracteriza al hipertexto y es cómo navegamos la red, pero también puede suponer un problema de privacidad. Hoy en día, muchas imágenes y código embebido utiliza cookies y otros métodos para rastreaer nuestro comportamiento de navegación. Muchas veces para mostrar anuncios. Estos dominios se llaman "rastreadores de terceros".

Los cookies de internet son, esencialmente, archivos de texto que un sitio almacena en tu computadora para, en posibles visitas posteriores, "recuerda" información como tu idioma preferido o tus datos de inicio de sesión.

La plataforma de Ciber-mujeres no utiliza cookies ni ningún tipo de código de terceros.

Comunicaciones

Los sitios web que incluyen formularios de contacto deben describir por qué están pidiendo la información que piden y qué van a hacer con él después. Por ejemplo, si se va a utilizar para un boletín o una base de datos.

Ciber-mujeres no utiliza formularios de contacto. Tiene cuentas de correo asociadas al dominio para que las personas puedan contactar con el proyecto (contacto@cyber-women.com) y para solicitar información relacionada con aspectos de privacidad (privacy@cyber-women.com).

El servicio de correo de estas cuentas es administrado por Kéfir, proyecto que se compromete a implementar, día a día, medidas de seguridad, mantener -durante el menos tiempo posible, en este caso, una semana - historiales de la menor cantidad de información des-identificada (no asociada a individuos específicos) necesaria para que funcione el servicio.

Las cuentas de correo se acceden a través del webmail y clientes de correo, tomando en cuenta prácticas de seguridad mencionadas en la currícula.

Historiales y estadísticas web

Un 'log' es un registro. Los servicios y aplicaciones que se ejecutan en un dispositivo tienden a mantener algun tipo de registro. Esto brinda información para mejorar herramientas y solucionar potenciales errores. Generalmente, esta información es útil, pero puede llegar a incluir información personal como la dirección IP y nombres de usuarixs que puede ser usada para crear perfiles bastantes prcesisos acerca del comportamiento de personas. Por ello, es importante anonimizar los 'logs' de una manera segura. T

Lxs servidorxs de Kéfir no mantienen registro de direcciones IP, únicamente de visitas anonimizadas, los cuales borramos después de una semana.

Ciber-mujeres guarda estadísticas a través de https://sinpasis.kefir.red, una instalación propia de Kéfir de Piwik/Matomo[5]. Esto implica que sólo IWPR y Kéfir tienen acceso a estos datos. Hemos configurado Matomo para que no registre datos que pueda identificar a lxs navegantes, como las direcciones IP. Todos las visitas individuales se agregan para creatos datos genrealizados y se eliminan después de un mes. Matomo respeta la funcionalidad "Do-Not-Track" (no me rastrees) del navegador si unx navegante si no quiere que Matomo recolecte los datos no-personales de su visita.

Javascript

El sitio de Ciber-mujeres utiliza Javascript:

- zepto.min.js: Zepto[6] es una libreria minimalista de Javascript para navegadores modernos con compatibilidad con el API de jQuery
- agency.js: Ciber-mujeres se basa en el tema de Agency Jekyll[7]. Este javascript hace que el sitio funcione en dispositivos móviles.

Si deshabilitas javascript (por ejemplo, usando Tor Browser Bundle o cambiando la configuración de tu navegador), el sitio seguirá funcionando. En pantallas pequeñas, el menú aparecerá en el pie de página.

Cambios en esta política de datos

Este documento puede ser actualizado en el futuro. Regresa a esta página para ver cambios.

Contacto

Puedes remitir cualquier pregunta o duda relacionada con esta política de uso de datos a privacidad@cyber-women.com.

[5] https://matomo.org/
[6] https://zeptojs.com/
[7] https://github.com/y7kim/agency-jekyll-theme

Qué puedes hacer

Tú también puedes contribuir a tu privacidad. El hecho que, de nuestra parte, no recolectamos datos sin tu consentimiento, que cuando lo hacemos es por un tiempo limitado y de manera anonimizada y que no los compartimos con terceros más allá de dar un marco general por fines de rendición de cuentas a nuestras financiadoras, no quiere decir que haya otros intermediarios que estén vulnerando tu privacidad.

- Lee la currícula de Ciber Mujeres[8] e implementa prácticas más seguras ;)
- Instala el plugin Privacy Badger[9] en tu navegador web
- Configura tu navegador Firefox para deshabilitar el rastreo de navegación[10]

Cómo puedo cambiar mi configuración de cookies

La mayoría de los navegadores web te dan un poco de control sobre la mayoría de los cookies a través de la configuración del navegador. Para aprender sobre cookies, incluyendo cómo ver las que se habilitan y no, entra en https://aboutcookies.org o http://www.allaboutcookies.org/

Averigua cómo manejar cookies en los navegadores más conocidos:

- Google Chrome[11];
- Microsoft Edge[12];
- Mozilla Firefox[13];
- Microsoft Internet Explorer[14];

[8] https://cyber-women.com/es/#modulos

[9] https://www.eff.org/privacybadger/

[10] https://support.mozilla.org/en-US/kb/how-do-i-turn-do-not-track-feature

[11] https://support.google.com/accounts/answer/61416?co=GENIE.Platform%3DDesktop&hl=en

[12] https://privacy.microsoft.com/en-us/windows-10-microsoft-edge-and-privacy

[13] https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences

[14] https://support.microsoft.com/en-gb/help/17442/windows-internet-explorer-delete-manage-cookies

- Opera[15];
- Apple Safari[16].

Para más información relacionada con otros navegadores, visita el sitio web del equipo desarrollador del navegador. Para deshabilitar el rastreo de las Analíticas de Google, entra en https://tools.google.com/dlpage/.

[15]https://www.opera.com/help/tutorials/security/privacy/
[16]https://support.apple.com/kb/ph21411?locale=en_US