Guía de Ciberseguridad para Universitarias

CON EL FINANCIAMIENTO DE:

Unión Europea

Cooperación Española

EN COORDINACIÓN CON:

PUCP

unesco Cátedra

Este documento se ha realizado con la ayuda financiera de la Unión Europea y de la AECID. Las opiniones expresadas en el mismo no representan necesariamente la opinión oficial de la Unión Europea ni de la AECID.

Guía de Ciberseguridad para Universitarias

Contenido

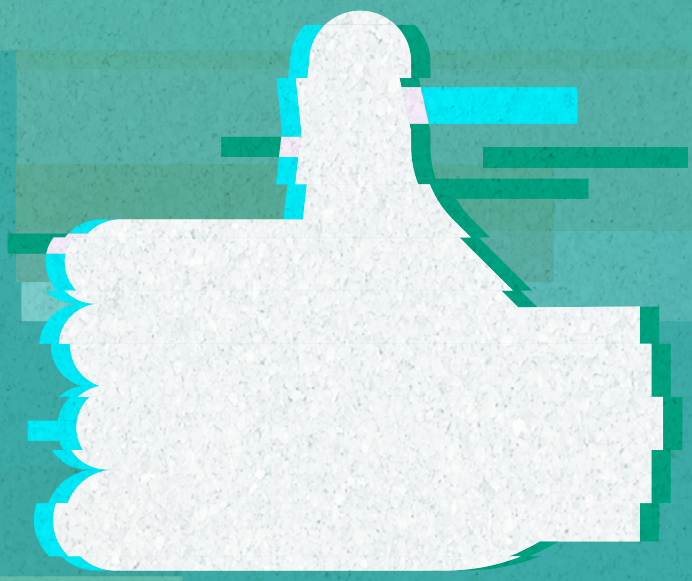
En un mundo cada vez más digital, en el que nuestras vidas se entrelazan con la tecnología, las mujeres universitarias peruanas viven a la vanguardia del cambio. Sin embargo, este mismo mundo digital que nos empodera, también se ha convertido en un terreno fértil para la violencia de género. Desde el acoso en línea hasta la difusión no consentida de imágenes, las amenazas virtuales acechan nuestras experiencias digitales. Este documento puede ser tu brújula para navegar por el mar digital, ya que te proporciona las herramientas y el conocimiento necesarios para proteger tu privacidad, tu seguridad y tu bienestar en línea. Aprenderás a identificar los riesgos, a prevenir situaciones peligrosas y a responder de manera efectiva ante cualquier forma de violencia digital.

¡QUE NO TE HACKEEN LA VIDA!

Esta guía es tu superpoder para navegar por el mundo digital sin miedo. Aprende a protegerte mientras luchas por tus derechos y los de tus amigxs.

¡Tu seguridad es lo más importante!

Capítulo 1:
Más allá de los likes



¿Sabías que la violencia de género también se esconde detrás de una pantalla? Al entender cómo se manifiesta en línea, podemos combatirla mejor y protegernos a nosotrxs mismxs y a nuestrxs seres más cercanxs. Vamos a desmenuzar los tipos de violencia de género más comunes en línea y detectar cómo nos pueden afectar.

Micromachismos digitales, ¿te suena?

De la vida real a las redes. Los micromachismos operan a través de la normalización de patrones culturales que perpetúan la desigualdad y el miedo. Por ejemplo:

- → **¡Se lo buscó!** ¡NUNCA! Esas frases son puro cuento para culpar a las víctimas y justificar la violencia de género.
- → **¡Debió tener más cuidado!** ¡Basta de culpar a la víctima! Es hora de acabar con esa mentalidad tóxica.
- → **Calladita te ves más bonita:** ¡Fuera estereotipos! Cada unx tiene derecho a expresarse como quiera.

Desigualdad conectada: la violencia estructural que nos limita en internet

La división del trabajo y los roles de género desiguales afectan nuestra presencia en el mundo digital y crean barreras para la participación plena de las mujeres y disidencias, como:

- → **Brecha digital de género.** La falta de acceso equitativo a la tecnología y la educación digital limita nuestras oportunidades para desarrollarnos profesionalmente y participar en la esfera pública.
- → **Falta de representación.** La falta de representación en puestos de liderazgo, en la creación de contenido y en la toma de decisiones en el ámbito digital perpetúa la desigualdad estructural.
- → **Acoso laboral en línea.** El acoso y la discriminación que sufren las mujeres y disidencias en el trabajo pueden trasladarse al entorno virtual a través de correos electrónicos, mensajes hostiles y plataformas de trabajo.

Violencia directa en línea

Esta categoría engloba todas las formas de agresión dirigidas específicamente hacia las mujeres y diversidades. Sus manifestaciones en línea pueden ser muy variadas:

- → **Acoso en línea o ciberacoso.** Mensajes amenazantes, insultos, persecución virtual, creación de perfiles falsos y/o publicación de información personal (conocido como "doxing") sin consentimiento son formas de violencia directa. También se presenta como una coordinación de ataques virtuales por parte de grupos con el objetivo de silenciar o dañar tu reputación.
- → **Difusión de contenido íntimo sin consentimiento o sextorsión.** La publicación de fotos o videos privados sin tu consentimiento es una forma grave de violencia que busca humillarte, controlarte o coaccionarte.
- → **Amenazas de violencia física o sexual.** ¿Te han amenazado con hacerte daño? Estos mensajes que te asustan y te hacen sentir en peligro son violencia pura y dura. Y además, tienen consecuencias que se pueden agravar con el tiempo.

El acoso en línea no es solo un problema de internet, es un reflejo de la sociedad machista en la que vivimos y que nos oprime. Para acabar con esto, es necesario cambiar las reglas del juego, necesitamos un mundo más justo para todxs.

Primera línea de defensa

Contraseñas seguras

Debemos enfatizar la importancia de utilizar contraseñas seguras para proteger nuestras cuentas en línea. Esto es importante para evitar que otrxs tengan acceso no autorizado a nuestros dispositivos y plataformas, protegiendo así la información personal que tenemos guardada.

Recomendaciones

- Combina siempre mayúsculas, minúsculas, números y símbolos. Mientras más extensa, mejor.
- No uses la misma contraseña en diferentes plataformas.
- Cambiar las contraseñas periódicamente, por ejemplo, cada mes o cada dos meses.
- Puedes usar un gestor de contraseñas para almacenarlas de forma segura. Algunos son Bitwarden, 1password, Nordpass.

Verificación en dos pasos (2FA): Tu escudo de defensa contra antiintrusxs

Imagina que alguien intenta entrar a tu cuenta sin tu permiso. ¡Felizmente, lo pensaste antes! La verificación en dos pasos es un sistema diseñado para dificultar el acceso no autorizado, incluso si alguien ya conoce tu contraseña. Este método te enviará un código único por mensaje de texto o correo electrónico que necesitarás para iniciar sesión además de tu contraseña. Si alguien intenta acceder a tu cuenta sin tu consentimiento, recibirás una alerta inmediata para que puedas tomar medidas y proteger tu información. Así estarás segurx.

¿"Phishing" y "malware"? ¿Qué es eso?

Como usuarixs digitales es necesario aprender ciertos conceptos del entorno digital además de conocer las amenazas y cómo se presentan, específicamente:

- → **Phishing.** Alguien intenta robar tu información personal para acceder a tus cuentas o dispositivos sin tu permiso.
- → **Malware.** Programa malicioso que puede dañar tu dispositivo y exponer información confidencial.

Estos tipos de ataques cibernéticos pueden comprometer la seguridad de tus dispositivos electrónicos y exponer información confidencial.

¿Qué puedes hacer?

- Instala un antivirus confiable en tu computadora.
- Mantén el sistema operativo y las aplicaciones actualizadas, tanto en tu computadora como en tu celular.
- No abras archivos o links de números o páginas desconocidas.

Respaldos (backups) para la preservación de datos

Imagina que tienes un álbum de fotos importantes y las guardas en una caja. Pero ¿qué pasaría si la caja se pierde o se daña? ¡Tus recuerdos estarían perdidos para siempre!

Un backup es una copia de seguridad de tus archivos importantes, como fotos, documentos y videos. De esta manera, si algo malo sucede con tu dispositivo o si lo pierdes, puedes recuperar tus archivos importantes desde la copia de seguridad.

Por esta razón, si tu dispositivo se ve infectado con un ransomware (software malicioso que bloquea el acceso a datos de tu dispositivo) o sufres el robo de tus dispositivos, los respaldos o backups regulares te darán la tranquilidad de no perder tus datos importantes.

Recomendaciones

- Realiza backups en diferentes dispositivos (discos duros externos, almacenamiento en la nube como Google Drive o iCloud).
- Sigue la regla 3-2-1. Son tres copias de la información: dos locales (USB y un disco externo) y una remota (la nube).

Wifi libre o público

Si bien el wifi libre es una red que te ofrece internet gratis en lugares públicos, te recomendamos evitar o limitar su uso si vas a revisar o intercambiar información sensible o personal. Las redes wifi gratuitas a menudo son inseguras, y hacen a tus dispositivos vulnerables al robo de información.

Precauciones

- Si debes usar una red wifi pública, utiliza una VPN (Red Privada Virtual) para encriptar o cifrar tus datos (hay opciones gratuitas), además de proteger tu identidad.
- No accedas a cuentas bancarias ni compartas información confidencial.
- Usa un antivirus.

Información adicional

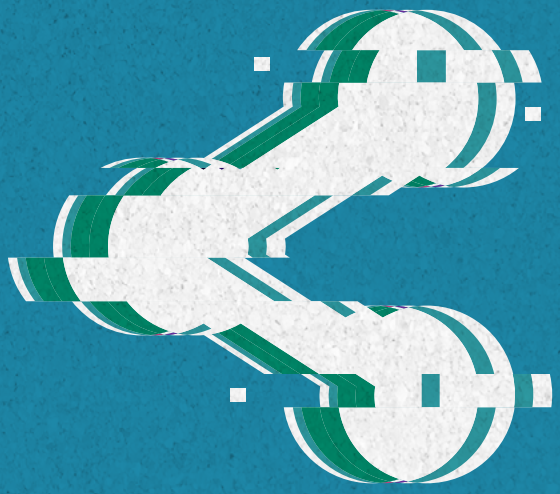
→ **Gestiona los permisos de aplicaciones.** Para controlar a qué información tienen acceso tus aplicativos.

→ **Bloqueo de pantalla.** Usa un código PIN, contraseña o datos biométricos para bloquear el dispositivo.

→ **Desactiva el Bluetooth y wifi cuando no lo uses.** Así te cuidarás de intrusxs que quieren obtener tu información con otros fines.

Recuerda que como usuarixs debemos adaptarnos y conocer las nuevas amenazas para protegernos.

Capítulo 2:
Dominando las redes



¡La información es poder! En la vida real, mujeres y disidencias a menudo tenemos que lidiar con un mundo machista y buscar herramientas para protegernos de ciertas situaciones. En el mundo digital esto se repite, pero ¿cómo nos defendemos? Hoy en día existen diversos manuales y fuentes de información feminista que nos pueden ayudar a gestionar y crear estrategias para ejercer el autocuidado en redes.

¿Cuáles son los riesgos y las amenazas?

La violencia de género en línea se manifiesta de diversas formas, como el acoso, la vigilancia, el robo de identidad y la difusión de información privada sin consentimiento. Reconocer estas amenazas es el primer paso.

Tu huella digital: lo que el internet sabe de ti

Debemos ser conscientes de que la información que compartimos en línea es de dominio público. La mayoría de aplicativos, al ser instalados, recopilan y almacenan tu información. La huella digital (el rastro que dejas al usar internet) puede revelar datos sensibles que podrían ser utilizados en contra de nosotrxs. Por eso, debemos tomar en cuenta:

- → No reveles todos tus datos personales. No es necesario compartir toda tu información personal (ubicación, dirección, número de teléfono o detalles financieros) en tus perfiles de redes.
- → Usar un alias o sobrenombre puede ayudar a protegerte.
- → No instales todo lo que te ofrezcan; limita la cantidad de aplicaciones en tu dispositivo.

¿Qué estoy compartiendo?

Reflexionando sobre todo aquello que compartes en línea.

- → **Evita publicaciones con información sensible de otras personas.** Proteger la privacidad de la comunidad y las personas con las que trabajamos, evitando la divulgación de información o los "repost" sin su consentimiento, además de la revictimización. Consulta siempre a la autora/x de una publicación antes de compartirla.

- → **Sé consciente del alcance de las publicaciones.** Podrías convertirte en tendencia de forma equivocada.
- → **Promueve la interacción positiva** y evita la propagación de discursos de odio, acoso o discriminación.

Ten presente que no estás solx

Si experimentas violencia o acoso en línea, estas son las formas de lidiar con esas situaciones que te sugerimos:

- → **Redes de apoyo.** Busca tu red de personas de confianza que puedan brindar apoyo emocional y práctico.
- → **Organizaciones y colectivas.** Acude a organizaciones o colectivas que conocen de violencia de género en línea para asesoramiento y recursos.
- → **Denuncia en la plataforma.** Reporta el acoso y la violencia en las plataformas de redes sociales, muchas cuentan con normas comunitarias.

Mensajería segura: ¿WhatsApp o Signal?

Entre los consejos que te presentamos aquí, es fundamental destacar la importancia de la seguridad en los servicios o apps de mensajería. Hoy en día, algunos de estos servicios han mejorado significativamente sus métodos; sin embargo, como ya lo hemos mencionado, la tecnología avanza y las formas de vulnerar dispositivos también.

WhatsApp: encriptación de extremo a extremo

WhatsApp es conocido por todxs, súper cómodo y fácil de usar, pero... ¡ojo! No es el más discreto. Tiene cifrado de extremo a extremo, es decir, los mensajes solo pueden ser leídos por el remitente y el destinatario. Además, dentro de las actualizaciones de seguridad ahora ya puedes enviar una foto y configurarla para que pueda ser visualizada una sola vez por el receptor, así como opciones para reportar spam, bloquear contactos y denunciar abusos en la misma aplicación. Ahora, imagina que WhatsApp es como una casa de cristal: todo lo que haces ahí puede ser visto, aunque no directamente por ti. WhatsApp también tiene la verificación en dos pasos, así que no dudes en utilizarla. Si a pesar de todo, WhatsApp es tu favorita ¡úsala con cuidado y siempre pensando en tu seguridad!

Signal: tu mejor aliadx feminista

Lxs expertxs en ciberseguridad nos dicen que esta app es segura y transparente, como un búnker digital donde tus conversaciones están a salvo de miradas indiscretas. Olvídate de los trolls tecno-

lógicos que quieren conocer todas tus acciones; con Signal tendrás el control total de tu información. Esta app es de código abierto, es decir, cualquier expertx en seguridad digital puede revisar y asegurarse de que sea lo más segura posible y hacer las actualizaciones necesarias. Dentro de sus funciones encontrarás la opción de autodestruir mensajes después de cierto tiempo, desactivar las capturas de pantalla y bloquear tu registro de llamadas. Además, Signal es una organización sin fines de lucro, lo que significa que no está motivada por intereses comerciales o publicidad.

De igual modo, toma en cuenta lo siguiente:

- Revisa periódicamente tu configuración de privacidad.
- Evita compartir información sensible.
- Considera eliminar mensajes confidenciales.
- Actualiza tu aplicación.
- Evita reenviar mensajes.

Consideraciones extra

Usa el código PIN para bloquear tu teléfono, contraseña o datos biométricos para evitar el acceso no autorizado a tu teléfono y a tus aplicaciones de mensajería.

Evita hacer clic en enlaces que te dicen que "ganarás 1000 dólares" o abrir archivos de remitentes desconocidos o sospechosos.

Autocuidado en Facebook e Instagram

Nuestra voz digital es tan poderosa como la que usamos en las calles; por eso, debemos cuidarla. Ahora te daremos algunas recomendaciones para proteger tus cuentas de Facebook e Instagram para seguir inspirando a miles.

Para una mejor comunicación con tus seguidorxs en cada una de estas plataformas, te recomendamos:

→ Muestra tu personalidad y comparte contenido original. La autenticidad genera conexión con tu audiencia, pero recuerda siempre que somos responsables de lo que comunicamos y cómo lo comunicamos.

→ Utiliza imágenes y videos atractivos que capten la atención y estén acorde con el tema de tu publicación.

→ Llamadas a la acción. Involucra a tus seguidorxs con preguntas, encuestas o peticiones para generar acciones concretas que nos beneficien colectivamente.

- → Difunde información de organizaciones y colectivas que brindan información feminista importante.
- → Permite un diálogo respetuoso en tus publicaciones. Elimina sin miedo los comentarios que busquen burlarse u ofenderte; no tienes por qué aguantarlos. Tu autocuidado es primero.

Tu seguridad al alcance de tus manos

¿Sabes cómo proteger realmente tus cuentas? Si estás empezando en el mundo del activismo feminista digital, es crucial saber cuidarte en plataformas como Facebook e Instagram.

Primero: Identifica los posibles riesgos

- → **Expresar opiniones políticas** en línea aumenta tu visibilidad en redes y podría atraer la atención de trolls, y es ahí donde podríamos convertirnos en blanco de acoso o vigilancia. Ten en cuenta que las publicaciones sobre manifestaciones o protestas pueden tener un alcance amplio, pero la información compartida podría ser utilizada fuera de contexto o con fines malintencionados.
- → **Los ataques coordinados** son amenazas comunes en esta labor. Se ha dado el caso de grupos privados de Facebook que han servido para coordinar un ataque a la cuenta de una persona con el fin de bloquear su cuenta o silenciarla. Lamentablemente, las normas comunitarias en Meta (empresa matriz de Facebook) hoy son deficientes.
- → **Vigilancia y monitoreo** por parte de gobiernos o entidades. Publicar información, fotos o videos durante tu participación o la de tus amigxs en manifestaciones podría ser utilizado para identificar, rastrear o tener acceso a detalles de organización interna de tu grupo o colectiva.

Segundo: ¿Qué hacer frente a los riesgos?

- → **Configura** quién puede ver tus publicaciones e información.
- → **Limita la visibilidad** de tu perfil y tus publicaciones para reducir el riesgo de exposición.
- → **Usa seudónimos o cuentas alternativas** para participar en actividades relacionadas con manifestaciones.
- → Si necesitas compartir información confidencial relacionada con una manifestación, **utiliza herramientas seguras** (como Signal o una VPN) para proteger tus comunicaciones.
- → **Riesgos legales.** Infórmate sobre las leyes y regulaciones locales relacionadas con las manifestaciones y las publicaciones en redes sociales en nuestro país.

Recuerda que la seguridad en línea es un proceso continuo que va cambiando según los avances tecnológicos. Por eso, debes estar atentx a cada cambio de la configuración de privacidad en la plataforma que usas.

Si de navegar segurx se trata...

→ **HTTPS:** La principal ventaja de HTTPS (protocolo de transferencia de hipertexto seguro) es que protege la información que se envía y recibe a través de internet. Además, generan más confianza en lxs usuarixs, ya que demuestran que se preocupan por la seguridad de sus datos.

Navegadores o motores de búsqueda seguros

Spoiler: No son Chrome ni Firefox.

→ **Tor.** El navegador conocido como Tor (The Onion Router) permite navegar de forma anónima, enmascarando la dirección IP y dificultando el rastreo de la actividad en línea. Sin embargo, no garantiza el anonimato absoluto y podrías tener más riesgo en la deep web, que alberga contenido ilegal y peligroso.

→ **Brave.** Bloquea automáticamente anuncios y rastreadores, lo que protege tu privacidad en línea. Sin embargo, su enfoque está más centrado en la experiencia del usuario y la velocidad. En comparación con Tor, es más lento. Igual es super seguro y tiene opción para la búsqueda de forma privada.

→ **DuckDuckGo.** Si buscas una experiencia de navegación más privada que la de Chrome, pero no necesitas el nivel máximo de anonimato que ofrece Tor, DuckDuckGo es una excelente opción.

Usa el modo incógnito sin dudar cuando te conectes desde un dispositivo que no es el tuyo.

VPN (Redes Privadas Virtuales)

Ya te hemos mencionado anteriormente a las VPN, que protegen tu privacidad y seguridad, especialmente en redes wifi públicas. Existen gratuitas y de pago; sin embargo, las gratuitas presentan limitaciones en cuanto a la velocidad y —en algunos casos— podría comprometer tu información. Te recomendamos PIA (Private Internet Access) y Proton VPN. Asimismo, Brave cuenta con VPN en su navegador.

Control de cookies y rastreadores

Para bloquear rastreadores de publicidad y sitios web puedes utilizar extensiones en tus navegadores, como Privacy Badger, Adblock Plus y U-block.

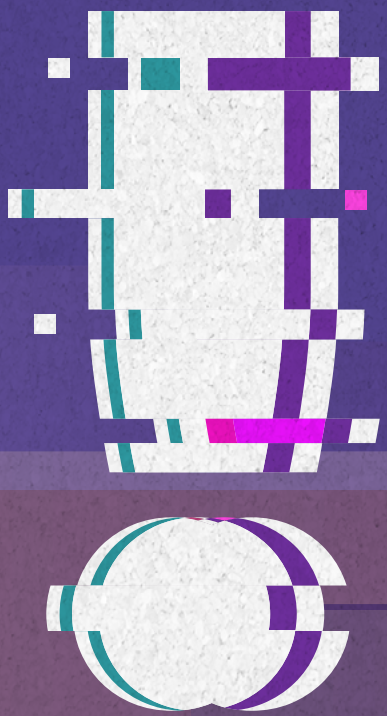
Correos electrónicos seguros

Para alta seguridad y privacidad considera el uso de ProtonMail o Riseup. Este último es muy popular en el activismo por la defensa de los derechos humanos.

Extras

- **Googléate.** Identifica cuáles de tus datos están disponibles públicamente y solicita su eliminación si es necesario.
- **Elimina de metadatos.** Imagina que tienes una foto en tu teléfono. Esa foto, además de la imagen en sí, guarda información extra que no se ve a simple vista, como la fecha en la que la tomaste, el lugar exacto, el modelo de tu cámara, hora, etc. Esas informaciones "invisibles" se conocen como **metadatos**. Eliminarlos ayudará a que esa información adicional no comprometa tu privacidad o seguridad. No obstante, en algunos casos, los metadatos son importantes porque nos ayudarán a obtener información relevante frente a un caso de desaparición de una persona, por ejemplo.
- **Eliminación segura de archivos.** Para eliminar archivos de forma segura de tu computadora puedes utilizar herramientas como Eraser o Ccleaner. Esto evitará su recuperación.

Capítulo 3:
Las violencias y mis redes de apoyo



Construir y cultivar **redes de apoyo** es un elemento fundamental para la seguridad y el bienestar de quienes somos activistas o trabajamos con temas de género.

Las redes de apoyo juegan un papel crucial frente a la violencia de género en línea porque permiten crear espacios seguros para sanar y crecer.

- **Busca a tus personas de confianza** que puedan escuchar, comprender y validar las experiencias vividas en línea. Esto ayudará a procesar emociones difíciles y reducir la sensación de aislamiento.
- **Escucha diferentes puntos de vista y consejos**. Compartir experiencias, preocupaciones y estrategias puede fortalecer la resiliencia individual y colectiva.
- **Encuentra tu fuente de motivación y aliento para continuar con el activismo** a pesar de los desafíos. Sentir el apoyo de otras personas que comparten los mismos valores y objetivos puede fortalecer la determinación y el compromiso.

Si estás pasando por una situación de violencia en línea, recuerda siempre que no estás solx, busca a tu amigx más cercanx.

¡Tu red es tu arma secreta para combatir la ciberviolencia!

Frente a las diferentes manifestaciones de violencia de género en línea es necesario conocer al enemigo y armar estrategias que puedan ayudar a tu colectiva o grupo a enfrentar estas situaciones. Entre las estrategias sugeridas están:

- **Difundir información** sobre nuevas amenazas, vulnerabilidades y estrategias de seguridad entre colectivas.
- **Consultar con ciberactivistas feministas o personas de confianza** con mayor conocimiento técnico digital. De este modo, puedes ayudar a otrxs a configurar herramientas de seguridad, resolver problemas y mejorar la protección de sus cuentas y dispositivos.
- **Coordinar respuestas** en caso de ataques coordinados, acoso o campañas de desprestigio, como la denuncia masiva de cuentas abusivas o la difusión de información para contrarrestar la desinformación.
- **Movilizar recursos o consultar con ONG.** Las redes de apoyo pueden ayudar a movilizar recursos para obtener apoyo legal, psicológico o técnico para quienes han sido víctimas de violencia digital.

Para una comunicación grupal segura, que no ponga en riesgo tu identidad y la de quienes forman parte de tu colectiva, puedes tomar en cuenta lo siguiente:

- → **Establece mecanismos de comunicación.** Por ejemplo: Si utilizas grupos en Facebook, te recomendamos poner como nombre de grupo algo totalmente inesperado a lo que se espera de ese grupo; así, pueden pasar desapercibidxs. Elijan a una sola persona o cuenta para gestionar el grupo. Lo ideal es que para estos fines uses correos electrónicos alternativos que no estén enlazados con tu correo personal.
- → **Fortalece tu grupo.** Demuestra tu compromiso con tu red y tu disposición a brindar apoyo.

Cuida tu mente

El activismo en línea es emocionalmente desafiante, poner límites frente a los desafíos es importante para nuestra salud mental.

- → **Prioriza tu autocuidado.** Te conoces mejor que nadie. Implementa estrategias para manejar el estrés, la ansiedad y la exposición a contenido negativo.
- → **Desconéctate cuando sea necesario.** Una desintoxicación digital regular es recomendada para proteger tu bienestar emocional.
- → **Considera la posibilidad de buscar terapia.** Si la experiencia en línea te afecta negativamente, hay profesionales que pueden atenderte. ¡Búscalxs!

Construyamos una experiencia en línea más segura y empoderada.

Reconociendo las violencias en línea

Identificar y reconocer la violencia sufrida es el primer paso para poder denunciar. Muchas veces, al mirar a nuestro alrededor y ver cómo se desarrolla la violencia estructural, podemos entrar en un estado psicológico que nos hace creer que nada puede cambiar la situación, lo que se convierte en un obstáculo importante para la denuncia. Sin embargo, debemos luchar frente a estas ideas.

- → **Valida lo que sientes.** Cuando algo se siente mal, probablemente lo sea, y es necesario actuar.
- → **Elimina las categorías absolutas.** No generalices con términos como “todo”, “nada”, “siempre” o “nunca”; enfócate en situaciones concretas.

→ **Aceptar el daño.** Reconocer el impacto de la violencia te permitirá enfrentar el dolor y avanzar hacia un proceso de sanación como sobreviviente.

Ser víctima, sobreviviente y sujeto de derechos

Un proceso de empoderamiento frente a las violencias implica transitar por tres etapas:

- **Víctima.** Implica reconocer el daño sufrido como algo ajeno y evitable. Esta etapa es crucial para poder denunciar la violencia.
- **Sobreviviente.** Se trata de convertirse en un agente de transformación social y exigir verdad, justicia y reparación para todas las víctimas.
- **Sujeto de derechos.** Supone haber alcanzado un estado en el que la violencia está ausente y todos los derechos son reconocidos y ejercidos sin restricciones.

¿Por qué a nosotrxs?

Las mujeres y la comunidad LGBTQ+ se enfrentan a riesgos de seguridad digital específicos debido a que la violencia de género encontró una nueva forma de manifestarse a través de internet, lo que empeora debido a los roles de género, los estereotipos y la discriminación sistémica.

→ **Ataques dirigidos a activistas y defensorxs.** Las razones por las que mujeres y personas LGBTQ+ pueden verse expuestas a ataques en línea es porque son especialmente vulnerables a la violencia digital debido a su trabajo de denuncia y su visibilidad. Abundan las historias en red sobre este tipo de violencia, en especial de las activistas, defensoras de derechos humanos y periodistas feministas, a quienes han buscado silenciar.

→ **El "terror sexual" y la restricción del espacio digital.** El "terror sexual" se impone por los patrones culturales y la violencia simbólica limita la libertad de las mujeres en el espacio digital. El miedo a la violencia nos lleva a evitar ciertos espacios, la autocensura y restringir nuestras actividades en línea, lo que impacta negativamente en nuestra seguridad digital, libertad y bienestar.

→ **Los trolls y los haters** no soportan que pensemos diferente o que defendamos nuestros derechos. Mujeres y personas LGBTQ+ ya llevamos un estigma por ser quienes somos. Y si además opinamos sobre política o luchamos por causas justas, podemos convertirnos en el centro de atención de lxs antiderechos.

→ **Los roles de género y estereotipos** juegan un papel fundamental en nuestro acceso a la tecnología y educación en seguridad digital. La falta de acceso a computadoras, dispositivos móviles y conocimientos nos hace más vulnerables a los riesgos en línea.

- → **Manipulación emocional.** Las mujeres son socializadas para ser cuidadoras y compasivas, lo que puede dificultar en la capacidad para establecer límites y defenderse en línea. Esta socialización puede hacernos más propensxs a ser víctimas de estafas, phishing y otros.
- → **Ineficacia de operadores de justicia.** La falta de una perspectiva feminista en la respuesta institucional a la violencia de género implica que la violencia en línea no se aborda con la seriedad y atención que se merece.
- → **Normalización de la violencia.** La violencia de género en línea, así como en la vida real, está normalizada, lo que dificulta que quienes la sufren puedan identificarla, denunciarla y buscar ayuda.

Las mujeres enfrentan riesgos de seguridad digital específicos debido a la intersección de la violencia de género en línea, los roles de género, los estereotipos y la discriminación sistémica. Es fundamental abordar estos problemas desde una perspectiva de género, promoviendo la educación en seguridad digital, fortaleciendo la respuesta institucional y desafiando las normas culturales que perpetúan la violencia.

Identificando la violencia de género en línea

Para aprender a reconocer y comprender la violencia de género en línea, debemos estar atentxs a lo siguiente:

- → **Mensajes amenazantes o humillantes.** Recibes mensajes que te hacen sentir insegurx, te atacan por tu género o te amenazan con daño físico o emocional. Estos mensajes pueden ser anónimos, seudónimos o con nombre propio.
- → **Control y vigilancia.** Esto no solo es exclusivo de cuentas de terceros o desconocidos; una forma de violencia de género en línea también la encuentras cuando tu pareja o expareja intenta controlar tus actividades en línea, te espían o exigen acceso a tus cuentas como un mecanismo de control o aislamiento.
- → **Difusión no consentida de imágenes íntimas.** Alguien comparte tus fotos o videos privados sin tu consentimiento. Debes tener en cuenta que, en nuestra regulación penal actual, ya se considera actualmente la manipulación de imágenes con IA (inteligencia artificial) para la sextorsión.
- → **Acoso constante.** Recibes una gran cantidad de mensajes no solicitados, llamadas o correos electrónicos de naturaleza sexual o hostil.
- → **Ciberacoso.** Eres objeto de burlas, comentarios pasivo-agresivos, insultos o rumores en línea, lo que puede afectar tu reputación y bienestar emocional.

¿Y si quiero denunciar?

El ordenamiento jurídico peruano sanciona la violencia de género. Sin embargo, aún existe mucho desconocimiento y falta de capacitación de los operadores de justicia frente a las modalidades que se dan en el ámbito digital. En este tipo de situaciones te recomendamos comunicarte con alguna organización o colectiva que pueda brindarte apoyo, darte luces sobre cómo responden o han respondido nuestrxs operadorxs frente a casos similares, con el fin de que puedas analizar la situación con la información que tener un panorama más completo.

En principio, la violencia de género en línea es denunciable, pero para iniciar este proceso podrías considerar lo siguiente:

- → **Asociaciones y colectivas feministas.** Elabora una lista de enlaces a asociaciones feministas que pueden brindar apoyo e información sobre violencia de género en línea.
- → **Instituciones y recursos.** Contacta instituciones y recursos, como el teléfono de atención a víctimas de violencia de género (Línea 100 del Ministerio de la Mujer y Poblaciones Vulnerables), o haz tu denuncia en una comisaría, lo que no es siempre recomendado: aunque es tu derecho y la policía debe recibir tu denuncia, a veces no existe gente capacitada para atenderte sobre este problema específico.
- → **Material didáctico.** Busca enlaces a material didáctico sobre la violencia de género en línea.

Hiperderecho es una organización que se dedica a promover y defender los derechos digitales en el Perú. Su trabajo se centra en brindar asesoría legal, capacitación y recursos a personas y organizaciones que enfrentan desafíos en el ámbito digital. Puedes revisar su información en: www.hiperderecho.org

Recuerda: Denunciar la violencia de género es un acto de valentía y un paso importante para romper el ciclo de la violencia en sus diversas formas de expresión.

¿Qué acciones puedes tomar?

Frente a una situación de violencia de género en línea, lo mejor que puedes hacer es:

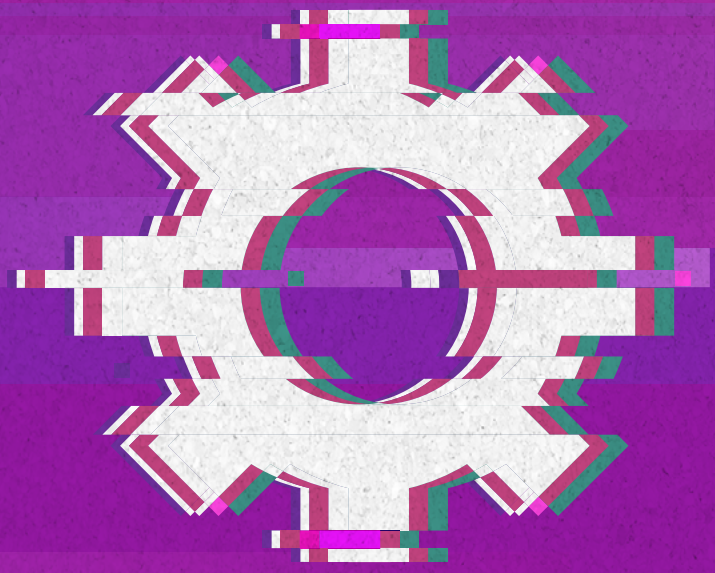
- Grabar o documentar, recopilar fotos y capturar mensajes o correos electrónicos.
- Si es posible, identifica al agresor y recopila toda su información (nombre de usuarix, dirección IP, etc.).
- Registra cuándo ocurrieron los hechos para facilitar la investigación.
- Indica en qué redes sociales o aplicaciones se produjo la violencia.

Ten presente que, para todo proceso legal, las pruebas son cruciales y te ayudarán en tu defensa. Es fundamental estar informadx, evaluar riesgos, implementar las medidas de seguridad adecuadas y buscar apoyo cuando sea necesario.

¿Qué hacer después de denunciar?

- **Guarda todas las pruebas.** No elimines ninguna evidencia, ya que podría ser necesaria para la investigación.
- **Busca apoyo.** Habla con familiares, amigxs de lucha o unx profesional de la salud mental sobre lo que estás pasando.
- **Sigue el proceso.** Mantente informadx sobre el avance de tu caso y participa en las diligencias que se te soliciten.

Capítulo 4:
Rompiendo el código



¡No todo puede recaer en nosotrxs! Si nos cuidamos y protegemos está bien, pero recordemos que se trata de un trabajo conjunto. ¿Qué puedes hacer además de usar las recomendaciones anteriores?

- → **Exigir responsabilidad a las empresas.** Debemos informarnos, revisar y exigir el cumplimiento de las normas de comunidad de las redes sociales y plataformas, y abogar por mejores procesos de denuncia y respuesta ante la violencia digital.
- → **Combatir la desinformación.** Siempre debemos verificar las fuentes de información antes de compartir o denunciar contenidos que promuevan la violencia, la discriminación o el odio.
- → **Compartir conocimientos y experiencias.** Es importante fomentar la educación en seguridad digital, compartir buenas prácticas y crear espacios de aprendizaje para fortalecer la seguridad colectiva.

Es necesario hablar del enfoque integral que combina la responsabilidad individual, la colaboración colectiva y la acción comunitaria para crear un entorno digital más seguro y protegido para todas las personas.

Estrategias para hackear el patriarcado digital

Si eres parte de una colectiva u organización o trabajas por los derechos digitales de forma independiente, es importante la planificación de una estrategia de seguridad digital eficaz:

1. **Ficha de documentación de incidentes.** Esta herramienta sirve para registrar los incidentes de seguridad digital que hayan ocurrido, como el acoso, el phishing o el acceso no autorizado a dispositivos. Aquí también puedes documentar la evidencia e identificar patrones de abuso para diseñar estrategias de prevención. Es importante utilizar la ficha inmediatamente después de un incidente para capturar detalles relevantes.

2. **Modelo de riesgos.** Este modelo ayuda a evaluar las amenazas digitales a las que te enfrentas junto con tu organización o colectiva. Por su naturaleza, debe actualizarse periódicamente para reflejar los cambios en el panorama de seguridad digital. Este proceso implica lo siguiente:
   - → **Identificar los activos a proteger.** Determinar la información o los datos críticos para la organización y que deben ser protegidos.
   - → **Identificar al enemigo.** Analizar quiénes podrían estar interesadxs en atacar a la organización y sus motivaciones.

- → **Evaluar la capacidad de lxs adversarixs.** Comprender los recursos y las habilidades de lxs adversarixs para determinar el nivel de sofisticación de las amenazas.
- → **Identificar las amenazas.** Enumerar los posibles ataques o incidentes que lxs adversarixs podrían llevar a cabo.
- → **Medir el riesgo.** Evaluar la probabilidad de que una amenaza se concrete y el impacto potencial en la organización.

Un paso adelante de las amenazas

El plan de seguridad digital establece las acciones concretas que se tomarán para abordar las amenazas identificadas en el modelo de riesgos. El plan debe considerar:

- → **Medidas reactivas.** Acciones para responder a incidentes que ya han ocurrido, como el cambio de contraseñas o la restauración de datos.
- → **Medidas proactivas.** Acciones para prevenir futuros incidentes, como la capacitación en seguridad digital, la configuración de la privacidad en redes sociales o la implementación de herramientas de seguridad.

El plan debe ser adaptado al contexto específico de la organización, y debe equilibrar la conveniencia, el costo y la privacidad.

Armando un protocolo

El protocolo define un conjunto de medidas de seguridad digital que aplicaremos de forma sistemática a actividades o procesos específicos dentro de la organización. El protocolo debe:

- → **Identificar las amenazas y riesgos específicos.** Analizar las vulnerabilidades y fortalezas de la organización frente a cada amenaza.
- → **Establecer acciones para mitigar los riesgos.** Definir los pasos a seguir para prevenir o responder a cada amenaza.
- → **Asignar responsabilidades.** Determinar quiénes son lxs responsables de implementar las medidas de seguridad.
- → **Establecer un plan de monitoreo.** Definir cómo se evaluará la efectividad del protocolo y cómo se realizarán las actualizaciones.

El protocolo de seguridad digital debe ser revisado y actualizado periódicamente para adaptarse a los cambios en el entorno digital y las necesidades de la organización.

Resumen

Conceptos clave

- → **Activismo.** Participación en causas sociales o políticas utilizando las TIC como herramienta para la expresión, organización y movilización.
- → **Ciberseguridad.** Se refiere al uso seguro y responsable de las tecnologías de la información y la comunicación (TIC). Esto incluye computadoras, internet, dispositivos móviles y cualquier herramienta que almacene, comparta o reciba información.
- → **Mitigación de amenazas.** Implica tomar medidas para reducir los riesgos digitales mediante la educación, la implementación de herramientas de seguridad y la creación de políticas institucionales.
- → **Riesgos digitales.** Lxs activistas, especialmente las mujeres universitarias, enfrentan riesgos específicos en línea, como el acoso, la vigilancia, el robo de identidad y la censura.

Criterios para una Guía de Ciberseguridad en tu casa de estudios

1. Conocimiento y conciencia

- **Comprende el panorama digital.** Es fundamental que sepas cómo funcionan las TIC, las plataformas digitales y los riesgos asociados a su uso.
- **Identifica amenazas específicas.** Reconoce las amenazas particulares que enfrentan las mujeres universitarias activistas, como el acoso en línea con enfoque de género y la vigilancia por parte de actores estatales o no estatales.
- **Conoce el marco legal.** Debes estar informada sobre las leyes y regulaciones relevantes para la ciberseguridad, el activismo en línea y la protección de datos.

2. Herramientas y estrategias

- **Privacidad y seguridad en redes sociales.** Domina la configuración de privacidad en redes sociales como Facebook, Twitter e Instagram. Así, limitarás el acceso no consentido a la información personal y protegerás la identidad.

- **Contraseñas seguras y autenticación de dos factores.** Implementa contraseñas fuertes y únicas para cada cuenta utilizando gestores de contraseñas, y activa la autenticación de dos pasos para mayor seguridad.
- **Uso de software de seguridad.** Instala y utiliza antivirus, antimalware y firewalls para proteger los dispositivos de amenazas digitales.
- **Comunicaciones seguras.** Utiliza herramientas de comunicación encriptada, como Signal o WhatsApp con cifrado de extremo a extremo, para proteger la privacidad de las conversaciones.
- **Navegación segura.** Emplea navegadores que prioricen la privacidad, como Tor o Firefox con configuraciones de privacidad avanzadas, y utiliza VPN para enmascarar la dirección IP y la ubicación.
- **Respaldo de datos.** Realiza copias de seguridad periódicas de la información importante para prevenir la pérdida de datos en caso de ataques o fallos técnicos.

3. Políticas y protocolos

- **Códigos de conducta.** Establece códigos de conducta claros para el comportamiento en línea dentro de la comunidad universitaria, incluyendo el uso responsable de las redes sociales y la prevención del ciberacoso.
- **Políticas de ciberseguridad.** Las universidades deben desarrollar políticas integrales que aborden la ciberseguridad en todos los niveles, incluyendo la protección de datos, la gestión de riesgos y los protocolos de respuesta a incidentes.
- **Protocolos de respuesta a incidentes.** Define procedimientos claros para reportar, investigar y responder a incidentes de ciberseguridad y ciberacoso, incluyendo la designación de un coordinador de ciberseguridad.

4. Empoderamiento y autocuidado

- **Cultura de ciberseguridad.** Fomenta una cultura proactiva de ciberseguridad entre las mujeres universitarias, promoviendo la responsabilidad individual y colectiva.
- **Redes de apoyo.** Crea redes de apoyo entre estudiantes para compartir información, recursos y experiencias sobre ciberseguridad.
- **Autocuidado digital.** Prioriza el bienestar mental y emocional en el entorno digital, aprendiendo a manejar el estrés, la ansiedad y la sobrecarga informativa.

Glosario

A

Activos: En el contexto de la seguridad digital, los activos son la información o los datos que una organización o individuo desea proteger. Esto puede incluir información personal, datos de contacto, estrategias de campaña, registros de donantes, etc.

Adversarios: Individuos o grupos que buscan comprometer la seguridad de los activos. Pueden ser exparejas, acosadores en línea, grupos de odio, entidades gubernamentales u otras organizaciones. Más conocidos como el enemigo, trolls, invasores.

Acoso coordinado en redes sociales: Se refiere a acciones conjuntas en línea por parte de múltiples individuos con el objetivo de hostigar, silenciar o desacreditar a una persona u organización. Puede incluir el uso de perfiles falsos, la difusión de información falsa, la denuncia masiva de cuentas y las amenazas de violencia.

B

Backup: Copia de seguridad de datos importantes almacenada en un lugar separado del dispositivo principal, para proteger contra la pérdida de datos en caso de ataques, fallos técnicos o robo de dispositivos.

C

Certificado de seguridad: Documento digital que verifica la identidad de un sitio web y permite una conexión encriptada (HTTPS) entre el navegador y el servidor.

Ciberpatriarcado: Término utilizado para describir la extensión de las estructuras patriarcales y la violencia de género al espacio digital.

Cifrado: El proceso de convertir información legible en un código ininteligible para protegerla del acceso no autorizado. El cifrado de extremo a extremo garantiza que solo el remitente y el receptor puedan leer los mensajes.

D

Dominio: La dirección de un sitio web, como "google.com" o "facebook.com". Es importante para las organizaciones proteger su dominio para evitar suplantaciones o la creación de sitios web falsos que imiten su identidad.

E

Espacio vital: En el contexto de la autodefensa feminista, el espacio vital se refiere al espacio físico alrededor de una persona que necesita para sentirse segura. Invadir el espacio vital de una persona puede ser una forma de intimidación o agresión.

F

Fase de arrepentimiento (falso arrepentimiento): Una etapa en el ciclo de la violencia donde el agresor puede disculparse, prometer cambiar o mostrar afecto para manipular a la víctima y mantener

el control. Es importante reconocer que este arrepentimiento a menudo no es genuino y que el ciclo de violencia puede repetirse.

Ficha de documentación de incidentes: Herramienta para registrar detalles sobre incidentes de violencia o acoso en línea, incluyendo la fecha, la hora, la plataforma, la descripción del incidente y las acciones tomadas. La documentación de incidentes ayuda a identificar patrones de abuso y puede ser útil para reportarlos ante las plataformas o autoridades.

G

Gestor de contraseñas: Programa que genera y almacena contraseñas seguras para múltiples cuentas en línea. Ayuda a lxs usuarixs a crear contraseñas fuertes y únicas sin tener que memorizarlas todas.

H

HTTPS: Protocolo de comunicación que cifra la información transmitida entre el navegador y el servidor, protegiendo los datos de ser interceptados. Los sitios web seguros que utilizan HTTPS se identifican con un candado verde en la barra de direcciones del navegador.

Huella digital: Los rastros de datos que una persona deja en línea a través de su actividad en sitios web, redes sociales, aplicaciones y otros servicios digitales. La huella digital puede ser utilizada para rastrear, identificar y perfilar a lxs usuarixs.

I

Indefensión aprendida: Estado psicológico en el que una persona cree que no tiene control sobre las situaciones y que sus acciones no tendrán ningún efecto, lo que puede llevar a la pasividad y la resignación frente a la violencia.

Ingeniería social: Técnicas de manipulación psicológica utilizadas para engañar a las personas y obtener información confidencial, como contraseñas o datos bancarios.

M

Malware: Software malicioso diseñado para dañar, deshabilitar o acceder a un sistema informático sin el consentimiento del propietario.

Metadatos: Información adicional almacenada en archivos digitales que puede revelar detalles sobre el autor, la fecha de creación, la ubicación y las modificaciones realizadas. Los metadatos pueden utilizarse para identificar a las personas y rastrear su actividad.

Modelo de riesgos: Proceso para identificar, analizar y evaluar los riesgos potenciales a la seguridad digital. Ayuda a las organizaciones a comprender las amenazas a las que se enfrentan y a priorizar medidas de protección.

P

Phishing: Técnica de engaño en la que lxs atacantes se hacen pasar por entidades confiables para obtener información confidencial, como contraseñas o datos bancarios. Los ataques de phishing a menudo se realizan a través de correos electrónicos o mensajes que parecen legítimos.

Pre-violencia: Comportamientos o señales de advertencia que pueden preceder a la

violencia física, como la intimidación, el control, las amenazas verbales o la invasión del espacio personal.

Protocolo de seguridad digital: Conjunto de reglas y procedimientos establecidos por una organización para proteger sus datos y sistemas. Los protocolos de seguridad pueden incluir políticas de contraseñas, directrices para el uso de dispositivos y planes de respuesta a incidentes.

R

Red de apoyo: Grupo de personas de confianza que pueden brindar apoyo emocional, práctico o legal a las víctimas de violencia o acoso en línea.

Resiliencia: Capacidad de una persona para superar la adversidad, el trauma o la violencia y recuperarse de las experiencias negativas.

S

Seguridad digital: Medidas y prácticas utilizadas para proteger la información, los datos y los sistemas informáticos de accesos no autorizados, uso indebido o daños.

Servidor: Computadora que proporciona servicios o recursos a otros dispositivos en una red. Las organizaciones pueden alojar sus sitios web, correos electrónicos y otros servicios en servidores.

Sobreviviente: Persona que ha experimentado violencia o trauma y ha comenzado el proceso de recuperación y empoderamiento.

Sextorsión: Forma de chantaje o extorsión en la que una persona es amenazada con la difusión de imágenes o videos íntimos si no cumple con ciertas demandas.

T

Terror sexual: El miedo constante que experimentan las mujeres a ser víctimas de violencia sexual, lo que limita su libertad de movimiento y sus elecciones.

Tor: Red de servidores voluntarios que permite la navegación anónima en línea, lo que dificulta el rastreo de la actividad del usuario.

V

Verificación en dos pasos (2FA): Medida de seguridad que requiere dos métodos de autenticación para acceder a una cuenta en línea. Generalmente, esto implica una contraseña y un código enviado a un dispositivo móvil o una aplicación de autenticación.

Violencia estructural: Violencia que se deriva de las normas sociales, las instituciones y las estructuras de poder que perpetúan la desigualdad y la discriminación, como el patriarcado.

Violencia simbólica: Violencia que se ejerce a través de patrones culturales, lenguaje, imágenes y representaciones que refuerzan la desigualdad y la discriminación.

VPN (Red Privada Virtual): Tecnología que cifra el tráfico de internet y enmascara la dirección IP del usuario, proporcionando mayor privacidad y seguridad en línea.

Bibliografía

- AARP (2010). Social Media and Technology Use Among Adults 50+. Washington DC: AARP.
- Campione, R. (2020). La plausibilidad del Derecho en la era de la inteligencia artificial: filosofía carbónica y filosofía silícica del Derecho. Madrid: Dykinson.
- Cerrillo, A. (2009). "Comentarios a la Ley 11/2007". En E. Gamero y J. Valero (coords.), *La ley de administración electrónica. Comentarios a la Ley 11/2007*, 2.ª ed. (pp. 757 y ss.). Aranzadi.
- Fernández Rodríguez, J. J. (2021). "El fortalecimiento democrático como garantía frente a los riesgos de seguridad del siglo xxi". En J. J. Fernández Rodríguez (coord.), *Democracia y seguridad: respuestas para avanzar en el sistema público* (pp. 149 y ss.). Tirant lo Blanch.
- Giant, N. (2014). *Ciberseguridad para la i-generación Usos y riesgos de las redes sociales y sus aplicaciones*. Madrid: NARCEA, S.A. DE EDICIONES.
- Hobbs, C. y Torreblanca, J. I. (2020). *La soberanía digital de Europa*. Catarata.
- Moret, V. (2018). "Un nuevo escenario jurídico para la ciberseguridad en España: el Real Decreto Ley 12/2018, de Seguridad de las redes y sistemas de información". *Diario La Ley*, 11 de octubre de 2018.
- Parisier, E. (2017). *El filtro burbuja. Cómo la web decide lo que leemos y lo que pensamos*. Taurus.
- Periano, M. (2019). *El enemigo conoce el sistema. Manipulación de ideas, personas e influencias después de la economía de la atención*. Taurus.
- Piñar Mañas, J. L. (dir.). (2016). *Reglamento europeo de protección de datos. Hacia un nuevo modelo europeo de privacidad*. Reus.
- Robles Carrillo, M. (2021). *Seguridad en redes 5G: la acción de la Unión Europea. XVI RECSI*. Lérida.
- UIT (2018). *Sentando las bases para la 5G: oportunidades y desafíos*.

Otros recursos

- Ballesteros Moffa, L. A. (2020). *Las fronteras de la privacidad: el conflicto entre seguridad pública y datos personales en una sociedad amenazada y tecnológica*. Comares.
- ENISA (2019). *Threat Landscape for 5G Networks*.

Documentos oficiales

- "La lucha contra las amenazas híbridas - Una respuesta de la Unión Europea" (JOIN 2016, 18).
- "Aumentar la resiliencia y desarrollar las capacidades para hacer frente a las amenazas híbridas" (JOIN 2018, 16).
- "Proteger Europa de ciberataques e interrupciones a gran escala: Aumentar la preparación, seguridad y resistencia" [COM (2009) 149, de 30 de marzo].
- Comunicación relativa a la protección de infraestructuras críticas de información "Logros y próximas etapas: hacia la ciberseguridad global" [COM (2011) 163, de 31 de marzo].
- Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco).
- Directiva 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.
- Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre la ENISA (Agencia de la Unión Europea para la Ciberseguridad) y sobre la certificación de ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) N° 526/2013 (Reglamento de Ciberseguridad).
- Reglamento (UE) N° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

Recursos web

- *Electronic Frontier Foundation.* (s.f.). *Autoprotección Digital Contra La Vigilancia: nuestra guía avanzada para protegerte a ti y a tus amigos del espionaje en línea*. https://ssd.eff.org/es/
- https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2021/Enero/Noticia-2021-01-29-primer-estandar-espanol-UNE-evaluacion-ciberseguridad-productos-TIC.html
- https://guiasbib.upo.es/ciberseguridad/definicion#:~:text=La%20segurida d%20inform%C3%A1tica%2C%20tambi%C3%A9n%20conocida,seguros%2 0y%20tecnolog%C3%ADas%20que%20pueden
- https://hiperderecho.org/wp-content/uploads/2022/01/Fanzine-acuerpandonos-1.pdf
- https://hiperderecho.org/wp-content/uploads/2024/08/Agravamiento-de-penas-y-persecucion-de-discursos-en-internet.pdf
- https://hiperderecho.org/wp-content/uploads/2024/04/kit_Internet-Disidente.pdf
- https://hiperderecho.org/tecnoresistencias/wp-content/uploads/2019/01/violencia_genero_linea_peru_2018.pdf

- https://www.dsn.gob.es/es/actualidad/sala-prensa/estrate-gia-seguridad-nacional-2021
- https://www.lamoncloa.gob.es/consejodeministros/ referencias/paginas/2007/ refc20071102.aspx#InfraCr%C3%ADticas
- https://www.ontsi.red.es/es
- Protege.LA. (s.f.). Guías de Seguridad Digital. https://protege.la/guias/
- Todas las guías de ciberseguridad feminista de Proyecto Aurora Autoprotección Digital Contra La Vigilancia: nuestra guía avanzada para protegerte a ti y a tus amigos del espionaje en línea. https://ssd.eff.org/es/