#DigitSafe

Boosting digital safe spaces and resilience

Manual de resiliencia digital

Co-funded by the Erasmus+ Programme of the European Union

#DigitSafe

“#DigitSafe-Boosting digital safe spaces and resilience” aims at empowering young people to become resilient and safe digital citizens, enabling them to address some of the challenges and negative impacts of the digital era.

Project partners:

CONEXX-EU

inova aspire

CESUR
Tu Centro Oficial de FP

alma radio 101.9

Co-funded by the
Erasmus+ Programme
of the European Union

Introducción

El proyecto **#DigitSafe-Boosting digital safe spaces and resilience** siguiendo la Estrategia de Juventud de la UE 2019-2017 en línea con el Objetivo 4 de Juventud de la UE "Información y Diálogo Constructivo" pretende empoderar a los jóvenes para que se conviertan en ciudadanos digitales resilientes y seguros, permitiéndoles hacer frente a algunos de los retos e impactos negativos de la era digital.

El proyecto **#DigitSafe** persigue fomentar un conocimiento más amplio y profundo entre los jóvenes sobre los dos temas clave de la ciberseguridad y el discurso de odio y la seguridad y la privacidad, en particular entre los grupos de jóvenes más vulnerables, construyendo espacios y prácticas digitales comunes más seguros, así como impulsando sus capacidades en términos de resiliencia digital.

Este proyecto también quiere alcanzar los siguientes tres objetivos principales específicos:

- **Promover la ciudadanía digital entre los jóvenes** de los países participantes, de conformidad con la Estrategia de la UE para la Juventud 2019-2027, proporcionándoles información práctica y recopilada sobre Seguridad y Privacidad, Discurso de odio y Ciberacoso.
- Proporcionar a los jóvenes, especialmente a los que tienen menos oportunidades y a menudo carecen de conocimientos básicos sobre información y datos, las competencias necesarias para mejorar su **resiliencia digital**.
- Desarrollar una metodología innovadora que traduzca la información relevante recopilada en un único manual en una **campaña de concienciación pública multicanal**, utilizando las prácticas y el lenguaje, las herramientas y las tendencias de comunicación audiovisual más comunes entre los jóvenes. Una estrategia multimedia y multicanal que explote la gran cantidad de posibilidades de creación de contenidos accesibles a todos los usuarios que ofrece el panorama actual de las redes sociales, dirigida a reforzar la capacidad de los jóvenes para tomar decisiones racionales, conociendo sus derechos digitales.

Este Manual de resiliencia digital sobre Ciberacoso, Discurso de odio, Seguridad y Privacidad ofrecerá de forma exhaustiva y unificada orientación, información práctica (recursos

jurídicos, recursos psicológicos, consejos, recursos de aprendizaje abierto y otros recursos de formación) y recomendaciones clave sobre diferentes cuestiones para que los jóvenes adquieran un conocimiento más profundo de sus derechos, riesgos digitales y amenazas en el contexto de estos temas. Aumentará la concienciación sobre las oportunidades y los recursos disponibles para desarrollar habilidades que permitan afrontar los problemas derivados de la vida digital actual de los jóvenes. Capacitará a los jóvenes para convertirse en ciudadanos digitales comprometidos y fomentará un mundo digital más seguro. Recopilará una gran cantidad de información, unificándola de forma más útil y completa.

Este Manual se dividirá en dos módulos:

1. **Ciberacoso & discurso de odio**
2. **Seguridad & Privacidad**

Proporcionará información no sólo sobre el marco jurídico, la sensibilización y la prevención, sino que también ofrecerá directrices de actuación, así como consejos y recomendaciones.

1. Cyberbullying

1. CIBERACOSO

1.1 ¿Qué es el ciberacoso?

A nivel europeo, se han encontrado múltiples definiciones de ciberacoso que incorporan unos u otros aspectos en función de las características específicas de cada uno de los países en los que se ha realizado el estudio (Bélgica, Bulgaria, Países Bajos y España). Sin embargo, el estudio desarrollado en 2016 por el Departamento de Derechos de los Ciudadanos y Asuntos Constitucionales perteneciente al Parlamento Europeo "Cyberbullying among Young People" ha elaborado una definición bastante precisa y homogénea que puede ser utilizada transnacionalmente en la Unión Europea.

"El ciberacoso describe aquellas situaciones en las que el acoso tiene lugar en Internet, principalmente a través de teléfonos móviles y redes sociales. El ciberacoso corresponde, por tanto, a un acto igualmente agresivo e intencionado, llevado a cabo mediante el uso de las tecnologías de la información y la comunicación (TIC)."

Al igual que el acoso fuera de línea, el ciberacoso suele implicar a los siguientes 3 participantes clave: la conducta debe producirse intencionada y repetidamente y debe haber un desequilibrio en las relaciones de poder entre el agresor y la víctima:

1. **El agresor**. Persona que lleva a cabo la agresión.
2. **La víctima**. Persona que sufre la agresión.
3. **Los espectadores**. Aquellos que ven lo que ocurre entre el acosador y la víctima, pero no están directamente implicados en el acoso.

En relación con las personas implicadas, es importante destacar que existe una diferencia importante entre el acoso y el ciberacoso y es que el agresor (el acosador) puede permanecer en el anonimato en el caso del ciberacoso, puede esconderse bajo una identidad falsa (o la identidad de otra persona) e incluso pueden ser varias personas las que se escondan detrás de esta identidad. No obstante, el ciberacoso deja un rastro electrónico que puede servir como prueba y como medio para poner fin a este comportamiento. Desgraciadamente, a pesar de estas diferencias, el acoso cara a cara y el ciberacoso suelen darse en paralelo.

Además, existen características clave del ciberacoso que facilitan su identificación y comprensión:

El ciberacoso es malicioso y nunca accidental. El ciberacosador tiene el objetivo claro y consciente de dañar a la víctima, causarle dolor, humillarla, hacerla sufrir física o mentalmente.

Se realiza desde una posición de poder. El ciberacosador siempre tiene ventaja y ocupa una posición de superioridad. Dependiendo del entorno en el que se produzca el ciberacoso, puede tratarse de un ciberacoso en grupo contra una víctima que está sola. Asimismo, los agresores pueden aprovecharse de una víctima no agresiva o vulnerable, incapaz de defenderse.

Se dirige repetidamente a intimidar, enfadar o avergonzar a las víctimas. Una acción agresiva aislada aún no es Ciberacoso. Se convierte en Ciberacoso cuando la agresión se repite una y otra vez contra la misma persona (o las mismas personas).

La digitalización ha multiplicado los canales a través de los cuales se puede perpetrar el acoso a través de Internet. Sin embargo, algunas de las formas más comunes en las que se ataca a las víctimas de ciberacoso son las siguientes:

- **Redes sociales**
- **Plataformas de comunicación**
- **Plataformas de juegos**
- **Teléfonos móviles**

Para aclarar qué acciones entrarían dentro del Ciberacoso, he aquí algunos ejemplos que entrarían dentro de estas acciones ilegales:

- Difundir mentiras o publicar fotos/vídeos embarazosos de alguien en las redes sociales.
- Enviar mensajes ofensivos o amenazas a través de plataformas de comunicación.
- Enviar mensajes maliciosos bajo la identidad de otra persona.

1.2. Conozca la importancia del ciberacoso y sus consecuencias. Concienciación y cómo identificarlo:

Identificar el ciberacoso

Una forma clave de abordar el ciberacoso es ser capaz de identificarlo y estar atento a las señales de alarma. No existe una definición universalmente aceptada de ciberacoso a nivel internacional o europeo. Sin embargo, la Comisión Europea define el ciberacoso como:

'Acoso verbal o psicológico reiterado llevado a cabo por un individuo o un grupo contra otros a través de servicios en línea y teléfonos móviles.'[1]

Según el Consejo de Europa, el ciberacoso se distingue de otros tipos de acoso por el riesgo de exposición pública, las complejas funciones de los observadores y el tamaño de la audiencia que conllevan las tecnologías digitales y la comunicación.[2]

WiredSafety, el mayor grupo de seguridad, educación y ayuda en línea del mundo, no está de acuerdo con la propuesta de que el ciberacoso deba ser " repetido" para ser clasificado como ciberacoso. Por el contrario, puede que algunos incidentes graves de ciberacoso no necesiten repetirse para ser considerados ciberacoso. Por ejemplo:

- La sextorsión, el sext-bullying y los ataques significativos a la reputación (por ejemplo, los relacionados con la preferencia sexual, la actividad sexual y otros tipos de ataques a la reputación constitutivos de difamación).

- Amenazas de muerte o amenazas de daños corporales graves al objetivo o a alguien cercano al objetivo, diseñadas para angustiar al objetivo.[3]

Para crear un mundo en línea más tolerante y seguro, el ciberacoso debe abordarse a mayor escala, tanto a nivel individual como organizativo.

Según un informe de 2016 del Parlamento Europeo, la participación directa de los niños en el desarrollo de soluciones y políticas relacionadas con el ciberacoso ha sido econocida como uno de los métodos más eficaces para hacer frente a este problema.[4] Además, un informe de 2017 para el Consejo de Europa, concluyó que para hacer frente al ciberacoso, las voces de los jóvenes deben estar representadas y ser escuchadas a nivel europeo y nacional.[5] Está claro, por tanto, que las voces de los jóvenes deben estar en primera línea de estos debates.

Las consecuencias del ciberacoso no pueden tomarse a la ligera ni considerarse simples bromas, ya que no sólo se niegan las emociones y el sufrimiento de la víctima, sino que se

---

[1] 'Cyberbullying among Young People', Directorate General for Internal Policies (European Parliament), 2016, p.8.
[2] https://www.coe.int/en/web/campaign-free-to-speak-safe-to-learn/preventing-bullying-and-violence [accessed 27/05/2022)
[3] Bullying, Perspectives, Practices and Insight, ancie Richardson, Elizabeth Milovidov, Roger Blamire, Council of Europe (2017)
[4] Cyberbullying among Young People', Directorate General for Internal Policies (European Parliament), 2016, p.11
[5] Bullying, Perspectives, Practices and Insight, ancie Richardson, Elizabeth Milovidov, Roger Blamire, Council of Europe (2017) p.44

normaliza este tipo de violencia en el entorno digital. Las consecuencias del ciberacoso pueden ser duraderas y afectar a las víctimas de muchas maneras. En algunos casos extremos, el ciberacoso puede llevar incluso al suicidio. El Consorcio #DigitSafe ha llegado a estas conclusiones tras una intensa investigación llevada a cabo a nivel europeo en cuatro países y los testimonios de víctimas de ciberacoso recogidos por el proyecto. Redes Sociales y Ciberacoso entre Adolescentes desarrollado por el CCI ha ayudado a comprender el alcance de las consecuencias del ciberacoso en las víctimas que lo sufren. Podríamos destacar como principales consecuencias del Ciberacoso:

- **Consecuencias mentales y emocionales**

Las víctimas pueden sentirse tristes, avergonzadas, apenadas, estúpidas, deprimidas, enfadadas y ansiosas. Las víctimas suelen perder el interés por las cosas que antes les gustaban, desarrollan una baja autoestima o se sienten aisladas, incapaces de comunicarse con sus compañeros. A veces, las víctimas del ciberacoso pueden convertirse en "víctimas-agresores", reproduciendo el comportamiento y acosando a otros.[6]

En otras palabras, existe la posibilidad real de que el ciberacoso cause un profundo daño psicológico a las víctimas. Las víctimas del ciberacoso son[7]:

1. Más propensas a sufrir **depresión** y **ansiedad**.
2. Más propensas a **sufrir bajo rendimiento académico y problemas de conducta en la escuela.**
3. Los estudiantes que sufren violencia e intimidación tienen más probabilidades de tener **dificultades para desarrollar competencias democráticas básicas como la empatía, el respeto por los demás, la apertura a otras culturas y creencias, la tolerancia y la autoeficacia.**

- **Consecuencias físicas**

[6] Joint Research Centre (2013). Social Networks and Cyberbullying among Teenagers. https://publications.jrc.ec.europa.eu/repository/handle/JRC80157
[7] https://www.coe.int/en/web/campaign-free-to-speak-safe-to-learn/preventing-bullying-and-violence [accessed 27/05/2022)

Debido al estrés y la ansiedad que sufre la víctima, esto puede provocar **problemas físicos**, como sensación de cansancio por alteraciones del sueño o experimentar verdaderos **síntomas de salud**, como dolores de estómago o de cabeza.

- **Consecuencias legales**

La sensación de estar siendo ridiculizado o acosado por los demás impide a menudo a las víctimas del ciberacoso denunciar o tratar de solucionar el problema. Esto, unido a la lenta evolución en la tipificación legal del delito, hace que a menudo quede impune y favorece la repetición de los ataques.

Concienciar sobre el ciberacoso para prevenirlo es esencial. El primer paso para identificar el ciberacoso es tener una definición clara de lo que implica. Además, en Europa, para prevenir el ciberacoso se han tomado decisiones políticas y se han definido y puesto en marcha numerosos programas. Sin embargo, el impacto que tiene este fenómeno hace necesario que las instituciones europeas sigan investigando, legislando y fomentando acciones colectivas e individuales para hacerle frente.[8]

Dirigido a los jóvenes

El Centro de Investigación del Ciberacoso[9] El Centro de Investigación del Ciberacoso ha elaborado una serie de consejos estructurados sobre cómo proceder para prevenir el Ciberacoso y asegurarnos como usuarios. La prevención es siempre la mejor opción para luchar contra este problema. Además, hemos seleccionado estos consejos precisamente porque la mayoría de ellos tienen parámetros mucho más orientados a los niños que a los adultos jóvenes:

- **Mantenerse al día con la configuración de privacidad**

Los sitios y programas de redes sociales modifican y actualizan con frecuencia su configuración de privacidad. Asegúrate de familiarizarte con las nuevas opciones de perfil y mantén toda la información posible restringida a aquellas personas en las que realmente confías.

[8] Rizza C, Martinho Guimaraes Pires Pereira A. Social Networks and Cyber-bullying among Teenagers. EUR 25881. Luxembourg (Luxembourg): Publications Office of the European Union; 2013. JRC80157

[9] Cyberbullying Research Center. (2021.)Preventing Cyberbullying: Top Ten Tips for Adults Who Are Being Harassed Online

- **Restringir el acceso a su información de contacto**

No facilite tu correo electrónico ni tu número de teléfono a personas que no conozca. Además, mantén tu correo electrónico y tu número de teléfono fuera de las redes sociales. Nunca se sabe quién puede tener acceso a ellos y no se puede confiar en todos los "amigos" o "seguidores".

- **Aprender el protocolo de Internet**

Para evitar posibles problemas con otros internautas, aprende las convenciones sociales relacionadas con la interacción en el ciberespacio. Por ejemplo, no escriba todo en mayúsculas. Algunos pueden percibirlo como un grito. Resístase también a utilizar el sarcasmo en línea, ya que puede malinterpretarse fácilmente.

- **No envíes fotos o vídeos inapropiados.**

Recuerda que el novio o la novia de hoy puede ser el amante despechado de mañana. No querrás que alguien con fotos o vídeos tuyos inapropiados los cuelgue en Internet y los comparta con el resto del mundo. No te pongas en la situación de tener que preocuparte por esto.

- **Búscate a ti mismo en Google**

Siempre debe saber lo que se dice de usted. A menudo es sorprendente encontrar información que creías privada en bases de datos públicas, nuevos artículos o páginas de redes sociales indexadas por motores de búsqueda.

- **No aceptes solicitudes de amistad de desconocidos**

Si no conoces a la persona que te envía una solicitud de amistad o de seguimiento, ignórala. La mayoría de las redes sociales y aplicaciones también te dan la opción de bloquear al usuario si quieres.

- **Utiliza controles basados en el sitio**

Desactiva las opciones de búsqueda en determinadas redes sociales para evitar que el público en general te busque o te envíe mensajes. Esto te permite tener más control sobre con quién interactúas en línea, ya que eres el único que puede iniciarlo.

- **Mantenga protegida su información**

Si utilizas un ordenador o una red públicos inalámbrica, asegúrate de cerrar la sesión de cualquier sitio en el que estés cuando te alejes de ese ordenador, aunque sea por un minuto. De hecho, hazlo también en tus otros dispositivos móviles si existe la posibilidad de que alguien se acerque y utilice tu cuenta para hacer alguna gracia o travesura. No facilites las contraseñas a nadie y cámbialas con frecuencia. Además, asegúrate de que tu teléfono y tu tableta tienen un código de acceso y están bloqueados.

- **Sea escéptico en las interacciones en línea**

Incluso entre personas en las que confías, es arriesgado revelar demasiada información porque nunca sabes con seguridad si la persona con la que crees que te estás comunicando está realmente ahí... o si está sola.

- **Protégete a ti y a la gente**

Recuerda que algunas personas tienen mucho tiempo libre y lo único que quieren es hacer la vida imposible a los demás. No se lo permitas. Resístete a poner en Internet demasiada información personal o privada que pueda ser utilizada para acosarte o humillarte y resístete a interactuar con ellos de cualquier forma. Como indica la sabiduría convencional ¡No alimentes a los trolls de Internet!

<u>Dirigido a profesores y padres</u>

Es importante que las organizaciones, las escuelas, los lugares de trabajo y los individuos se comprometan a hacer frente al ciberacoso debido al impacto que este puede tener en las víctimas. La investigación desarrollada por el Cyberbullying Research Center en 2021 "Cyberbullying: Identificación, prevención y respuesta en 2021"[10] ofrece una amplia

[10] Hinduja and Patchin.(2021). Cyberbullying: Identification, prevention and Response: https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2021.pdf

explicación de cómo profesores y padres podrían abordar el ciberacoso en términos de identificación y prevención:

Educar a la comunidad sobre un uso responsable de los dispositivos centrado en la ciudadanía digital es quizá el paso preventivo más importante en lo que respecta a las instituciones educativas y sus profesores. Inculcar disciplina a los alumnos que se dedican a acosar o amenazar a otros y hacerles saber que lo que están haciendo es más que incorrecto, es un delito.

Es esencial incluir en varias áreas de los planes de estudio de las instituciones educativas contenidos en línea apropiados para debatir el ciberacoso entre otras amenazas digitales. Además, los mensajes podrían reforzarse en otras clases, especialmente en aquellas que utilizan tecnología y herramientas digitales. Establecer y reforzar un entorno de respeto e integridad en las instituciones educativas es crucial cuando las violaciones y el acoso se sacian formal o informalmente.

Además, desarrollar estrategias nuevas y creativas para luchar contra el ciberacoso es cada vez más importante hoy en día, sobre todo para hacer frente a formas menores de acoso y prevenirlas. Los investigadores Hinduja y Patchin (2021), del Cyberbullying Research Centre, dan diferentes ejemplos:

"Se puede pedir a los alumnos que creen carteles contra el ciberacoso para exponerlos por todo el colegio, o un vídeo de servicio público que transmita un mensaje contra el acoso o a favor de la amabilidad.

A los alumnos mayores se les puede pedir que hagan una breve presentación a los más jóvenes sobre la importancia de utilizar la tecnología de forma ética.

De lo que se trata aquí, una vez más, es de condenar el comportamiento (sin condenar al niño) al tiempo que se envía un mensaje al resto de la comunidad escolar de que el acoso, en cualquiera de sus formas, está mal y no será tolerado".[11]

En otras palabras, es importante no sólo para la educación formal, sino empezar a introducir en la educación formal en la escuela actividades no formales e informales para combatir y prevenir el Ciberacoso desde un punto de vista creativo.

[11] Hinduja and Patchin.(2021). Cyberbullying: Identification, prevention and Response: https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2021.pdf

Por otra parte, los padres "*deben demostrar a sus hijos con palabras y acciones que ambos desean el mismo resultado final: que cese el ciberacoso y que la vida no se haga aún más difícil...*".[12]

El Centro de Investigación sobre el Ciberacoso (https://cyberbullying.org/) subraya lo importante que es, como padres, no despreciar la perspectiva de sus hijos, sino validar su voz y su opinión. **Es fundamental que las víctimas del ciberacoso y los espectadores sepan que los adultos, al tener conocimiento de la situación de ciberacoso, "*intervendrán de forma racional y lógica, y no empeorarán la situación...*"**.[13]

¿Cómo deben reaccionar los padres si descubren que su propio hijo es un ciberacosador?

En primer lugar, deben explicarle cómo ese comportamiento provoca e inflige daño y dolor en el mundo real. Después, los padres deberían darle la oportunidad de seguir adelante y poner fin a ese comportamiento. Los investigadores Hinduja y Patchin (2021) proponen a los padres "*cultivar la empatía poniéndoles intencionadamente en situaciones que les incomoden y que puedan ablandarles el corazón*". Los niños necesitan saber que cada acción, aunque sea en línea, tiene consecuencias graves.

Por parte de los padres, es esencial empezar a prestar más atención al comportamiento y las acciones de sus hijos en Internet.

1.3. Directrices: ¿cómo tratar a las víctimas de ciberacoso? (Procedimientos, empatía, la importancia de escuchar, apoyo emocional, apoyo psicológico):

La recopilación de procedimientos y consejos sobre cómo proceder se ha conformado principalmente a partir de las propuestas más que cumplimentadas del Centro de Investigación sobre el Ciberacoso y Amnistía Jóvenes

(https://jeunes.amnesty.be/).

[12] Hinduja and Patchin.(2021). Cyberbullying: Identification, prevention and Response: https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2021.pdf
[13] Hinduja and Patchin.(2021). Cyberbullying: Identification, prevention and Response: https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2021.pdf

Cuando tú mismo eres la víctima

Si eres víctima, queremos aconsejarte con una serie de pasos a seguir si estás sufriendo ciberacoso:

- **Buscar ayuda**

¡En primer lugar, hay que hablar y discutir con familiares o profesionales!

- **Reportar el contenido**

Si el Ciberacoso se ha producido a través de una red social, denuncia el contenido a esa plataforma. Esto no siempre es efectivo, pero es importante que la red social sepa quién es el acusado para que pueda tomar medidas, a veces después de varias denuncias.

- **Protégete a ti mismo**

Cambia tu contraseña, aumenta la privacidad de tus publicaciones, elimina información personal como tu dirección de correo electrónico, número de teléfono o enlaces a otras cuentas.

- **Como medida temporal, elimina tu cuenta o cambia tu apodo.**

Intenta desconectarte de las redes sociales durante un tiempo, bloquea a la persona que es la fuente del ciberacoso.

- **Responde y recuerda a la persona que te acosa el marco legal señalándole que el acoso online es un delito penado por la ley.**

- **Si ocurre en el entorno laboral, habla con tu jefe.**

Informe a tu empleador si la persona que le acosa es un compañero de trabajo, o si el acoso se produce en un foro o blog relacionado con el trabajo. Si el acoso te impide hacer tu trabajo, tu empleador tiene que saberlo.

- **Cortaz lazos**

No te hagas amigo de quienes te tratan mal ni intentes que te caigan simpáticos. Si sientes que tienes que responder a la persona que te maltrata, hazlo con respeto. No intentes racionalizar o hacerte amigo de nadie que sea cruel con los demás.

- **No relacione**

Quienes acosan cibernéticamente quieren que reacciones. El problema es que, si respondes airadamente, el acosador puede alimentarse de esa respuesta y continuar con el ciberacoso (e incluso agravarlo). Además, tu respuesta puede tener consecuencias.

- **Póngase en contacto con el proveedor de servicios de Internet (ISP).**

Intente ponerse en contacto con el proveedor de servicios de Internet de la persona que le está acosando si ha sido identificada. El ISP puede entonces ponerse en contacto con la persona o tal vez cerrar directamente su cuenta de Internet.

- **Denuncia acudiendo a una comisaría de policía.**

Toma pruebas del ataque (por ejemplo, capturas de pantalla). La policía tomará nota de tu denuncia y de toda la información relacionada con ella y la plasmará en un informe. Te darán una copia del informe y un certificado de denuncia. A continuación, el informe se envía a la fiscalía, es decir, a los magistrados encargados de las investigaciones. Pida el número del informe para poder seguir el caso y saber qué fiscalía (de qué municipio) es competente.

- **Denunciar el ciberacoso públicamente.**

Comparte capturas de pantalla del acosador (asegúrate de ocultar el nombre de usuario y la foto de perfil del acosador para que no te acusen de difamación).

Como compañero (de trabajo o de estudios)

En este ámbito, Save the Children[14] ha señalado muy acertadamente algunas pautas sobre cómo actuar en caso de acoso escolar:

- Puedes sentir miedo o rechazo ante esta situación, pero actúa.
- This is not snitching; it is being supportive of those in need. Si ves que no puedes pararlo tú solo y que no es lo mejor, pide ayuda a un adulto o a un responsable. Esto no es chivarse, es ser solidario con quien lo necesita.

[14] Save the children. Advice for students on how to deal with bullying. https://www.savethechildren.es/publicaciones/consejos-para-estudiantes-frente-al-bullying-o-acoso-escolar

- Apoya al compañero acosado. Nadie se merece que le traten mal.
- Proponga la realización de cursos de formación o elabore materiales de sensibilización en su centro educativo o empresa para prevenir el ciberacoso y buscar ayuda.

Como profesor

Los profesores tienen que prestar atención a diferentes señales que pueden mostrar que un niño está siendo ciberacosado. Algunas de estas señales pueden ser un rápido aumento o disminución del uso del dispositivo o una respuesta emocional a lo que está sucediendo en su dispositivo. Si un niño esconde su pantalla o dispositivo cuando hay otros cerca y evita la discusión, esto debe tenerse en cuenta.

Además, los profesores también tienen que ayudar a los niños a identificar, responder y evitar el ciberacoso. Algunas directrices serían:

- La comunicación es muy importante, **así que, si alguna vez crees que un niño está siendo víctima de ciberacoso, habla con él en privado y pregúntale sobre ello.** También puedes hablar con uno de los padres sobre el tema. Los profesores pueden ser mediadores entre el niño, los padres y la escuela.
- **Promueva un entorno de clase seguro**. Ayude a los niños a desarrollar la inteligencia emocional para que adquieran conciencia de sí mismos y habilidades de autorregulación y aprendan a sentir empatía por los demás.
- Anima a los alumnos a prestar atención a las señales que pueden ayudarles a identificar cuándo ocurre algo en los medios digitales que les hace sentirse incómodos, preocupados, tristes o ansiosos.
- Enséñales a pensar antes de publicar.
- Explica a los alumnos las tres formas en que pueden y deben responder si son testigos de ciberacoso: si apoyas a la víctima del acoso eres un aliado, si intentas detener el ciberacoso eres un defensor y si eres víctima de ciberacoso tienes que denunciarlo a un adulto.

Como padres

Es muy probable que los niños no reconozcan que están siendo ciberacosados porque pueden sentirse avergonzados. Es muy común que los jóvenes sufran en silencio. Pueden tener miedo de que los padres reaccionen restringiendo su acceso en línea, pueden sentirse avergonzados por no poder ocuparse ellos mismos del acoso, pueden temer que los padres manejen las cosas de una manera que intensifique el acoso o que no entiendan el problema.

Por estas razones, si los padres observan algún signo en sus hijos deben actuar de inmediato. En primer lugar, **intente hablar con su hijo y escucharle**. La mejor forma de hacerlo es entablar una conversación con él/ella sobre lo que está pasando de forma calmada. Tómate tu tiempo para entender exactamente lo que ha pasado y el contexto en el que ha ocurrido. Es muy importante para tu hijo que no minimices la situación. Dado que las redes sociales se han convertido en una extensión de la vida cotidiana de los niños, un comentario o texto desagradable puede ser devastador para él/ella. Elogiar a tu hijo por haber hecho lo correcto hablándote de ello es una buena forma de aumentar la confianza entre vosotros dos.

Una vez que lo sepas, **ofrécele consuelo y apoyo incondicional**, ya que las víctimas de ciberacoso suelen experimentar un sentimiento de aislamiento. Demuéstrele a tu hijo que esta situación puede tratarse de una manera que no implique represalias en línea. Haga que su hijo se sienta seguro, debe ser la principal prioridad, así como hacerle saber que no es culpa suya.

Después, **intente reunir todas las pruebas posibles**. Imprima o haga capturas de pantalla o grabaciones de conversaciones, mensajes, fotos, vídeos y otros elementos que puedan servir como prueba clara de que su hijo está siendo víctima de ciberacoso. Lleve un registro de todos y cada uno de los incidentes para ayudar en el proceso de investigación. Asimismo, anote detalles relevantes como el lugar, la frecuencia, la gravedad del daño, la participación de terceros o testigos y los antecedentes.

El siguiente paso es **ponerse en contacto con el proveedor de contenidos**, ya que el ciberacoso siempre infringe las condiciones de servicio de todos los proveedores de servicios legítimos. Deberían tomar cartas en el asunto para que tu hijo no vuelva a sufrirlo.

Si el ciberacosador es un compañero de clase o va al mismo colegio que su hijo, **debe notificarlo al centro escolar lo antes posible**, ya que es posible que tengan normas para responder al ciberacoso. Los padres también pueden ponerse en contacto con la policía en caso de que la situación mencionada no ayude a mejorar.

Si es necesario, intente buscar asesoramiento para su hijo. Los niños pueden beneficiarse de hablar con un profesional de la salud mental. Es posible que prefieran dialogar con un tercero que pueda percibirse como más objetivo.

1.4. Medidas de prevención

No existe un método infalible para evitar que un niño sufra ciberacoso. Sin embargo, hay diferentes maneras de reducir la probabilidad de que sean el objetivo.

En primer lugar, **es importante utilizar contraseñas** para todo y no compartirlas con nadie. Una buena forma de mejorar la seguridad de los niños en Internet es utilizar las herramientas y ajustes de privacidad que ofrecen las redes sociales. Tenemos que asegurarnos de que los niños conocen los ajustes y herramientas de privacidad que ofrece la organización y revisar cada medio social y establecer los ajustes de privacidad en el más seguro. Esto significa hacer que las cuentas sean privadas, evitar que la gente les etiquete, etc.

Los niños tienen que saber que es importante mantener la privacidad de las cosas personales. Nunca deben compartir su dirección, número de móvil o dirección de correo electrónico en Internet. Deben tener cuidado con compartir demasiada información sobre a qué colegio van, sobre todo si tienen amigos o seguidores en Internet a los que no conocen muy bien.

T**ambién deben saber que tienen que cerrar la sesión cuando utilicen dispositivos públicos**, como ordenadores públicos o portátiles en el colegio o la biblioteca. Esto incluye cerrar la sesión de correo electrónico, cuentas de redes sociales, su cuenta escolar o cualquier otra cuenta que puedan abrir.

Por último, pero quizá lo más importante, **los niños deben ser conscientes de que si alguna vez son víctimas de ciberacoso deben denunciarlo a sus padres o profesores.**

1.5. Cómo denunciar el ciberacoso

(marco jurídico, instituciones, ONG, etc.)

Uno de los aspectos más significativos de la denuncia del ciberacoso es que la mayoría de los países europeos no cuentan con una legislación específica sobre el Ciberacoso. A pesar de la importancia, el gran número de casos y la preocupación entre los jóvenes, la legislación aún no ha avanzado en este ámbito. Esto ha hecho que la labor de instituciones y organizaciones sea esencial para ayudar a identificar los casos, denunciarlos y dar apoyo a las víctimas.

Bélgica

- **Marco jurídico**

El ciberacoso se considera una "infracción penal" en Bélgica, por lo que es objeto de sanción penal. No obstante, como en muchos otros países, no existe una ley penal específica en relación con el ciberacoso. Sin embargo, esto no significa que la infracción penal quede impune, sino que a través de otras leyes de Bélgica:

Art. 442 bis y art. 442 ter del Código Penal de Bélgica = Acoso.

"Quien diga mentiras perjudiciales en público que puedan dañar el honor o la reputación de otra persona comete una infracción del artículo 442 del Código Penal de Bélgica".

Art. 145.3 bis de la Ley de 13/06/2005 en relación con la comunicación electrónica, la difamación y la calumnia

Art. 448 del Código Penal de Bélgica= Insultos públicos

Art. 422 bis del Código Penal de Bélgica = Stalking (acoso)

Art. 383 del Código Penal de Bélgica = Indecencia pública

En el mundo del trabajo, el ciberacoso es un fenómeno relativamente reciente e inexplorado, a pesar del uso omnipresente de las TIC en los entornos y modalidades de trabajo actuales Recientemente se han adoptado el Convenio de la OIT sobre la violencia y el acoso, 2019 (núm. 190), y la Recomendación núm. 206 que lo acompaña, que incluyen en su ámbito de aplicación la violencia y el acoso que se producen también a través de las comunicaciones relacionadas con el trabajo, incluidas las posibilitadas por las tecnologías de

la información y la comunicación. En Bélgica, estas disposiciones se incorporan a la legislación sobre seguridad y salud en el trabajo (SST).

- **Instituciones y ONG**

En Bélgica, si el ciberacoso se produce en un centro educativo, existen reglamentos y normas internos que permiten a estas instituciones imponer sanciones contra el mismo. Aparte de eso, hay algunas organizaciones y plataformas que dan apoyo y orientación a aquellas víctimas que buscan ayuda antes del proceso legal que, en la mayoría de los casos, es complejo, difícil y traumático para el joven.

CyberHelp (https://smartcity.brussels/news-750--the-cyberhelp-app-combats-cyberbullying)

Una iniciativa conjunta de la Policía Federal de Bélgica, la Universidad de Mons y la Federación Valonia-Bruselas. Se trata de una **app contra el ciberacoso**, para denunciarlo a través del propio smartphone. La app incluye un botón que les permite hacer una captura de pantalla de su historial de chat con un ciberacosador y un segundo botón a través del cual pueden enviar este contenido a las personas encargadas de tratar estas situaciones en su centro educativo. En 2021, el equipo de CyberHelp presentará la aplicación a 12.000 estudiantes mediante un centenar de visitas a colegios de Valonia y Bruselas.

Amnesty Jeunes Belgium (https://jeunes.amnesty.be/)

Télé-Accueil Bruxelles (https://tele-accueil.be/bruxelles/)

Télé-Accueil es un **servicio telefónico y de chat**. Quien desee "alguien con quien hablar" encontrará a través del número 107 un oído atento, gratuito, 24 horas al día, 7 días a la semana, en el anonimato y la confidencialidad. Es una gran opción para aquellas víctimas que, por vergüenza o incapacidad para saber cómo enfrentarse al ciberacoso, la ciberdelincuencia o los discursos de odio, reciben ayuda y una persona que les escucha y aconseja.

España

Cuando se produce ciberacoso hay varias cosas que debes tener en cuenta. En primer lugar, no respondas ni reenvíes mensajes de ciberacoso y bloquea a la persona que te acosa. Es importante guardar pruebas del ciberacoso. Registra las fechas, horas y descripciones del ciberacoso. Es posible denunciar el acoso tanto en la plataforma en la que se produce como legalmente, por ejemplo, a la policía.

Cuando denuncies a través de la plataforma, revisa primero sus términos y condiciones o las secciones de derechos y responsabilidades. Estos términos describen el contenido que es o no apropiado y, a continuación, denuncia el ciberacoso a la red social para que puedan tomar medidas contra los usuarios que abusen de los términos del servicio.

En cambio, cuando el ciberacoso implica amenazas de violencia, pornografía infantil o envío de mensajes o fotos sexualmente explícitos o acoso y delitos de odio, se considera delito. En estos casos, debe denunciarse a la policía.

Existen fundaciones que ofrecen apoyo y ayuda a aquellos niños o adolescentes y sus familias que no saben cómo abordar este tema o cómo denunciarlo. Por ejemplo:

Cybersmile (https://www.cybersmile.org/who-we-are)

Es una organización sin ánimo de lucro comprometida con el bienestar digital y la lucha contra todas las formas de acoso y abuso en línea.

AEPAE (https://aepae.es/plan-nacional)

Es una Asociación para la Prevención del Acoso Escolar en España. El objetivo de esta asociación es desarrollar conductas preventivas en niños y adolescentes encaminadas a la resolución de conflictos en el ámbito escolar.

INFOACOSO (https://infoacoso.es/telefonos-de-ayuda-contra-el-acoso-y-el-bullying)

Esta asociación ofrece en su web una guía sobre cómo actuar si estás siendo víctima de ciberacoso y dónde llamar para denunciarlo, según la comunidad de España en la que vivas.

Países Bajos

En los Países Bajos, las siguientes instituciones y organismos pueden ayudarte si eres víctima de ciberacoso:

- **MiND** (https://www.mindnederland.nl/) Línea directa sobre discriminación en Internet que registra y evalúa las denuncias de discriminación en la red.
- Diríjase al servicio antidiscriminación de su zona. Todos los municipios de los Países Bajos tienen un servicio antidiscriminación al que puede dirigirse para plantear una pregunta o una queja sobre discriminación.
- Llame al teléfono nacional de ayuda contra la discriminación (0900 235 5345).
- Póngase en contacto con la policía si le han acosado, intimidado, amenazado o algo peor.

Algunos de los servicios mencionados son específicos para quienes han sufrido discriminación. La discriminación suele definirse como el trato desigual a otra persona por razón de su etnia, sexo, género o características genéticas. La discriminación está prohibida por la legislación de la UE:

Artículo 21: "*Se prohíbe toda discriminación, y en particular la ejercida por razón de sexo, raza, color, orígenes étnicos o sociales, características genéticas, lengua, religión o convicciones, opiniones políticas o de cualquier otro tipo, pertenencia a una minoría nacional, patrimonio, nacimiento, discapacidad, edad u orientación sexual*.'[15]

Como el ciberacoso adopta muchas formas, puedes sentirte víctima de un ciberacoso que no sea específicamente discriminatorio. En estos casos, algunas sugerencias son:

- Denuncia el ciberacoso a la escuela/trabajo (si estás siendo acosado por alguien en tu lugar de educación/empleo).
- Stop Online Bullies es un plan holandés de intervención a medida para víctimas de ciberacoso con bajo nivel educativo, cuyo objetivo es enseñar a las víctimas a enfrentarse al ciberacoso y a sus efectos negativos.
- Bloquea y denuncia al ciberacosador en tus redes sociales.
- Bloquea y denuncia el número del acosador.

[15] Article 21 EU law: Non discrimination https://fra.europa.eu/en/eu-charter/article/21-non-discrimination#:~:text=EU%20Charter%20of%20Fundamental%20Rights,-Previous%20title&text=1.,2.

- Solicite información al departamento de policía local.
- Presente una denuncia oficial a la policía (si considera que es lo mejor tras hablar con el departamento de policía).

En los Países Bajos, las escuelas tienen responsabilidades específicas para combatir y prevenir el ciberacoso. Por ejemplo, el programa KiVa tiene como objetivo mejorar la seguridad de los alumnos en las escuelas y ha sido financiado con subvenciones del Ministerio de Educación Neerlandés.

El programa KiVa (https://www.kivaprogram.net/) es un programa antiacoso basado en la investigación y la evidencia finlandesa que fue desarrollado originalmente por la Universidad de Turku y se ha aplicado en escuelas de todo el mundo. Se basa en tres elementos principales: prevención, intervención y seguimiento.[16]

- **Prevención**. En las escuelas se aplican acciones preventivas como el plan de estudios KiVa para centrarse en la prevención del acoso escolar.

- **Intervención**. Las técnicas de intervención de KiVA se dirigen a los niños que han estado directamente implicados en el acoso. El objetivo es proporcionar a las escuelas y a los alumnos herramientas centradas en la solución.
- **Seguimiento anual**. Las encuestas anuales realizadas tanto a los alumnos como al personal de las escuelas KiVa se utilizan para supervisar la eficacia del programa y proporcionar información sobre cómo mejorar su labor contra el acoso.

De programas como KiVa pueden extraerse lecciones que pueden aplicarse a personas y organizaciones de todo el mundo. Es evidente que centrarse en medidas preventivas es crucial para garantizar que se abordan todas las formas de acoso. Esto puede aplicarse a los casos de ciberacoso mediante campañas educativas. Estas medidas garantizan que las personas puedan utilizar Internet de forma segura.

Bulgaria

Los ciberdelitos, incluidos el ciberacoso y los riesgos para la privacidad y la seguridad en línea, se denuncian al Departamento de Ciberdelincuencia del Ministerio del Interior de Bulgaria. Se trata de un mecanismo general de notificación de señales no urgentes de ciberdelincuencia (dedicado principalmente al ciberfraude y la pornografía infantil). El

[16] What is KiVa? https://www.kivaprogram.net/what-is-kiva/

programa está coordinado por el Departamento de Ciberdelincuencia (www.cybercrime.bg) de la Dirección General de Lucha contra la Delincuencia Organizada del Ministerio del Interior.

A través de un formulario en línea se puede denunciar el ciberacoso, el ciberfraude y la pornografía infantil. Para casos urgentes, se recomienda llamar al teléfono general de emergencias 112.

También existe un mecanismo gestionado por el Estado para apoyar y asesorar a niños y jóvenes sobre diferentes cuestiones, como el ciberacoso, los discursos de odio y los riesgos para la privacidad y la seguridad en línea. Este mecanismo es la **Línea Telefónica Nacional** para la Infancia 116 111 que gestiona y administra la Agencia Estatal de Protección de la Infancia con el objetivo de apoyar a todos los niños y sus familias en Bulgaria. Los operadores que atienden las llamadas son psicólogos formados que 24 horas al día, 7 días a la semana, de forma anónima y totalmente gratuita, están dispuestos a escuchar, apoyar, consultar y orientar a los llamantes sobre todas las cuestiones que les preocupan.

2. Discurso de odio

2. DISCURSO DE ODIO

2.1. ¿Qué es el discurso de odio?

No existe una definición universalmente aceptada del discurso del odio. En esta sección, esbozaremos un par de definiciones que se recogen tanto en la legislación de la UE como en las principales organizaciones que luchan contra la incitación al odio. El discurso de odio se define en la legislación de la UE como:

'*(Ilegal) La incitación pública a la violencia o al odio por razón de determinadas características, como la raza, el color, la religión, la ascendencia y el origen nacional o étnico*'

Aunque la Decisión Marco se refiere al racismo y la xenofobia, la mayoría de los Estados miembros han ampliado sus legislaciones nacionales para incluir otros motivos como la orientación sexual, la identidad de género y la discapacidad.[17] INACH (la red líder en la UE y a nivel mundial en la lucha contra el odio cibernético) define el discurso de odio como:

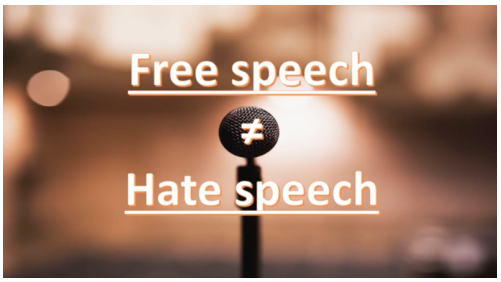
'*Las declaraciones públicas, intencionadas o no, discriminatorias y/o difamatorias; la incitación deliberada al odio y/o la violencia y/o la segregación basada en la raza, etnia, lengua, nacionalidad, color de piel, creencias religiosas o ausencia de ellas, género, identidad de género, sexo, orientación sexual, creencias políticas, estatus social, nacimiento, edad, salud mental, discapacidad, enfermedad, reales o percibidas, de una persona o grupo*.'[18]

La legislación de la UE protege la libertad de expresión, lo que lleva a algunos a pensar que existe un conflicto entre la protección de la libertad de expresión y la penalización del discurso del odio. Muchos expertos proponen que este supuesto "conflicto de intereses" entre la penalización del discurso del odio y la protección de la libertad de expresión está mal entendido.

De hecho, el Pacto Internacional de Derechos Civiles y Políticos prohíbe 'toda apología del odio nacional, racial o religioso que constituya incitación a la discriminación, la hostilidad o la violencia.'[19]

[17] Code of Conduct- Illegal Online Hate Speech Questions and Answers, (European Commission 2016) https://ec.europa.eu/info/sites/default/files/code_of_conduct_hate_speech_en.pdf
[18] INACH definition of hate speech https://www.inach.net/cyber-hate-definitions/
[19] ICCPR Article 20 (2)

Este breve vídeo explica con más detalle este concepto erróneo y por qué la libertad de expresión no es absoluta.



https://www.youtube.com/watch?v=V0HhyVLX0ZA

La "Pirámide del odio" (mostrada a continuación) representa el peligro de todas las formas de discurso del odio.[20]

La pirámide del odio se utiliza para ejemplificar cómo el discurso del odio ha sido históricamente (y sigue siendo) un precursor de la violencia extrema. Su objetivo es poner de relieve cómo el discurso del odio puede suponer una amenaza para los demás al contribuir a la pirámide del odio y la violencia. Combatir el discurso del odio, por tanto, es esencial para crear un mundo más pacífico y tolerante.

[20] https://www.rightsforpeace.org/hate-speech

2.2. Cómo prevenir los discursos de odio

El discurso de odio se aborda a nivel de la UE mediante la Directiva de Servicios de Comunicación Audiovisual (DSCA), que obliga a las autoridades nacionales de todos los países de la UE a garantizar que los servicios de comunicación audiovisual no contengan incitaciones al odio.[21] Además, a nivel de la UE, la Comisión acordó con Facebook, Microsoft, Twitter y Youtube un "Código de conducta para combatir la incitación ilegal al odio en línea". La aplicación de este código de conducta se supervisa periódicamente con una red de organizaciones de toda la UE.[22]

¿Cómo se puede prevenir el discurso del odio a nivel individual?

Una forma de combatir el discurso del odio es **bloquear y denunciar las cuentas de discurso del odio que encuentre en línea** (consulte la siguiente sección sobre consejos para denunciar el discurso del odio). Las Naciones Unidas recomiendan comprometerse con las siguientes prácticas para prevenir el discurso del odio[23]:

- **Haz una pausa**. Abstente de hacer comentarios de odio y/o de compartir ese contenido.
- **Comprueba los hechos**. Asegúrate de detectar información falsa y tendenciosa antes de difundir información errónea.
- **Desafía**. Difunde tu propio contra-discurso y desafía el discurso de odio siempre que sea posible.
- **Apoya**. Adopta una postura pública y extiende tu solidaridad a las víctimas del discurso del odio.
- **Denuncia**. Consulta las directrices comunitarias de las plataformas de medios sociales que utilices y denuncia los casos de discurso del odio que infrinjan estas directrices. En los casos más graves, puedes presentar una denuncia ante la policía (por ejemplo, cuando haya incitación a la violencia).

[21] Code of Conduct- Illegal Online Hate Speech Questions and Answers, (European Commission 2016) https://ec.europa.eu/info/sites/default/files/code_of_conduct_hate_speech_en.pdf
[22] The EU Code of Conduct on Tackling Illegal Hate Speech https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en
[23] United Nations- how to deal with hate speech? https://www.un.org/en/hate-speech/take-action/engage

- **Educa**. Comparte recursos educativos y campañas públicas o inicia conversaciones con tus amigos y familiares.

- **Comprométete**. Considera la posibilidad de unirte a una ONG o iniciativa que trabaje para hacer frente al discurso de odio dentro de tu comunidad.

Para saber más sobre el discurso de odio y las formas de prevenirlo, ponte a prueba respondiendo a este cuestionario de las Naciones Unidas: https://www.un.org/en/hate-speech/take-action/test-yourself

2.3. Cómo denunciar un discurso de odio

INACH es una red líder en la UE y en el mundo que trabaja para combatir el ciberodio. Es una fundación de derecho neerlandés con sede en Ámsterdam, pero cuenta con 32 miembros de 28 países. Su sitio web ofrece una plataforma en línea para denunciar cualquier incidente de ciberodio. Además de ofrecer un servicio de quejas y denuncias contra el ciberodio, INACH utiliza los datos de todas las denuncias recibidas para redactar informes y análisis. De este modo, intentan influir en la opinión pública, en las empresas de medios sociales y en las instituciones internacionales, lo que contribuye a su labor de presión en favor de una legislación internacional contra el ciberodio.

Además de denunciar casos de ciberodio a través de INACH, los usuarios también pueden denunciar directamente cualquier incidente de incitación al odio a través del canal de las redes sociales en el que lo encuentren. El sitio web del Consejo de Europa ofrece información sobre cómo denunciar en las redes sociales[24]. En algunos casos no es necesario tener una cuenta para denunciar.

Algunos países europeos han introducido procedimientos y mecanismos nacionales de denuncia de discursos de odio, delitos de odio y ciberacoso en el marco de la "Campaña Juvenil No al Discurso de Odio" del Consejo de Europa. Puedes consultar la lista de países y sus procedimientos de denuncia en el sitio web del Consejo de Europa[25]. Otras sugerencias para denunciar los discursos de odio son:

- Denuncie el discurso de odio a la policía.
- Informe a un organismo autorizado, por ejemplo, un tribunal civil o administrativo.

[24] Reporting on Social Media Channels https://www.coe.int/en/web/no-hate-campaign/reporting-on-social-media-platforms#{%2237117289%22:[]}
[25] https://www.coe.int/en/web/portal

- Denuncia a una ONG, por ejemplo, MiND es el centro nacional de denuncia de discursos de odio y contenidos discriminatorios de los Países Bajos.
- Habla con alguien de confianza, por ejemplo, un padre, un amigo o un profesor.

3. Ciberseguridad y privacidad

3. CIBERSEGURIDAD Y PRIVACIDAD

3.1.¿Por qué es importante la protección de los datos personales?

El término protección de datos personales se define en el Art. 4 (1) del Reglamento General de Protección de Datos:

'Los datos personales son cualquier información relacionada con una persona física identificada o identificable. Los nombres y las direcciones de correo electrónico son obviamente datos personales. La información sobre la ubicación, el origen étnico, el sexo, los datos biométricos, las creencias religiosas, las cookies de Internet y las opiniones políticas también pueden ser datos personales.'

En los próximos apartados profundizaremos en los tipos de datos que requieren protección.

La protección de datos es importante, ya que impide el uso indebido de la información de un individuo o de una organización, pretende prevenir diferentes riesgos para la privacidad y la seguridad, como actividades fraudulentas, piratería informática, suplantación de identidad y robo de identidad (descritos en la siguiente sección).

El tipo de datos que requieren protección

La información vital, como **nombres, direcciones, correos electrónicos, números de teléfono, información sanitaria o datos bancarios**, son datos que deben almacenarse y protegerse cuidadosamente. Si esa información cae en las manos equivocadas, puede comprometer la seguridad de las personas de muchas formas, como la integridad personal, la seguridad física y la seguridad financiera. La información robada también puede utilizarse para crear perfiles falsos y cometer fraudes. Algunos ejemplos de datos personales son:

- Nombre y apellidos
- Dirección del domicilio
- Una dirección de correo electrónico como name.surname@company.com
- Número del documento de identidad
- Datos de localización (por ejemplo, la función de datos de localización de un teléfono móvil)*.
- Dirección de protocolo de Internet (IP)

- ID de cookies*
- el identificador publicitario de tu teléfono
- datos en poder de un hospital o un médico, que podrían ser un símbolo que identifique de forma exclusiva a una persona.

Algunos ejemplos de datos que no se consideran personales son:

- Número de registro de la empresa
- Una dirección de correo electrónico como info@company.com
- Datos anónimos: los datos personales que se han convertido en anónimos de tal manera que el individuo no es o ha dejado de ser identificable ya no se consideran datos personales. Para que los datos sean realmente anónimos, la anonimización debe ser irreversible.

¿Quién es responsable de proteger nuestros datos?

La protección de datos es el proceso de salvaguardar información importante de la corrupción, el peligro o la pérdida. La importancia de la protección de datos aumenta a medida que la cantidad de datos creados y almacenados sigue creciendo a un ritmo sin precedentes.

Por lo tanto, las organizaciones que almacenan y gestionan información personal son responsables de garantizar que está a salvo de corrupción, compromiso o pérdida. En la Unión Europea, el Reglamento General de Protección de Datos (RGPD) (https://gdpr-info.eu/) protege los datos personales de los ciudadanos de la UE. Es la ley de privacidad y seguridad más estricta del mundo. Aunque fue redactado y aprobado por la Unión Europea (UE), impone obligaciones a las organizaciones de cualquier lugar, siempre que se dirijan a personas de la UE o recojan datos relacionados con ellas. El reglamento entró en vigor el 25 de mayo de 2018.

Elementos clave de la protección de datos

Un modelo de protección de datos muy importante es la tríada CIA, donde las tres letras del nombre representan los tres elementos de la protección de datos: *Confidencialidad, Integridad y Disponibilidad*. Este modelo se desarrolló para ayudar a individuos y organizaciones a desarrollar un enfoque holístico de la protección de datos. Los tres elementos se definen de la siguiente manera:

- Confidencialidad: Los datos sólo son recuperados por operadores autorizados con las credenciales adecuadas.
- Integridad: Todos los datos almacenados en una organización son fiables, precisos y no están sujetos a cambios injustificados.
- Disponibilidad: Los datos almacenados están disponibles de forma segura y rápida siempre que se necesiten.

Según el Reglamento General de Protección de Datos (RGPD), también existen varios principios de protección de datos personales que las organizaciones que los recopilan y gestionan deben cumplir:

- **Legalidad, equidad y transparencia**. El tratamiento debe ser lícito, justo y transparente para el interesado.
- **Limitación de la finalidad**. El responsable del tratamiento debe tratar los datos para los fines legítimos especificados explícitamente al interesado cuando los recopiló.
- **Reducción de los datos**. El responsable del tratamiento debe recoger y tratar sólo los datos absolutamente necesarios para los fines especificados.
- **Precisión**. El responsable del tratamiento debe mantener los datos personales exactos y actualizados.
- **Limitación de almacenamiento**. El responsable del tratamiento sólo puede almacenar datos de identificación personal durante el tiempo que sea necesario para los fines especificados.
- **Integridad y confidencialidad**. El tratamiento debe realizarse de forma que se garantice la seguridad, integridad y confidencialidad adecuadas (por ejemplo, mediante el uso de cifrado).
- **Responsabilidad**. El controlador de datos es responsable de poder demostrar el cumplimiento del GDPR con todos estos principios.

La importancia de la protección de datos aumenta a medida que la cantidad de datos creados y almacenados sigue creciendo a un ritmo sin precedentes. Además, hay poca tolerancia a los tiempos de inactividad que pueden imposibilitar el acceso a información importante.

Como se ha explicado anteriormente, las organizaciones que recopilan, almacenan y gestionan datos personales son responsables de garantizar que estos datos no se utilicen

indebidamente y estén disponibles para el personal autorizado en cualquier momento. El GDPR garantiza esto mediante requisitos legales concretos y sanciones para las organizaciones que no los cumplan. Por otro lado, los particulares pueden mantener la seguridad frente a intentos no deseados de terceros de acceder a sus datos, así como proteger su privacidad de aquellos con los que no consienten compartir su información personal.

3.2. Tipos de amenazas y delitos contra los datos personales y la privacidad

- **Robo de identidad**

El robo de identidad es **el delito consistente en obtener la información personal o financiera de otra persona para utilizar su identidad con el fin de cometer fraude**, como realizar transacciones o compras no autorizadas. El robo de identidad se comete de muchas formas diferentes y sus víctimas suelen sufrir daños en su crédito, sus finanzas y su reputación. El ladrón de identidad puede utilizar su información para solicitar créditos, declarar impuestos u obtener servicios médicos. Estos actos pueden dañar su situación crediticia y costarle tiempo y dinero restablecer su buen nombre.

El robo de identidad se produce cuando alguien roba su información personal, como su número de la Seguridad Social, su número de cuenta bancaria y los datos de su tarjeta de crédito. El robo de identidad puede cometerse de muchas formas distintas. Algunos ladrones de identidad rebuscan en los contenedores de basura en busca de cuentas bancarias y extractos de tarjetas de crédito. Otros métodos más tecnológicos consisten en acceder a bases de datos corporativas para robar listas de información de clientes. Una vez que los ladrones de identidad tienen la información que buscan, pueden arruinar la calificación crediticia de una persona y la situación de otros datos personales.

Los ladrones de identidad utilizan cada vez más la tecnología informática para obtener información personal de otras personas con fines de fraude de identidad. Para encontrar esa información, pueden buscar en los discos duros de ordenadores robados o desechados; piratear ordenadores o redes informáticas; acceder a registros públicos informatizados;

utilizar programas maliciosos de recogida de información para infectar ordenadores; navegar por sitios de redes sociales; o utilizar correos electrónicos o mensajes de texto engañosos.

Tipos de robo de identidad

Robo de identidad financiera

En el robo de identidad financiera, **alguien utiliza la identidad o la información de otra persona para obtener crédito, bienes, servicios o beneficios**. Esta es la forma más común de robo de identidad.

Robo de identidad en la Seguridad Social

Si los ladrones de identidad obtienen tu número de la Seguridad Social, pueden utilizarlo para solicitar tarjetas de crédito y préstamos y luego no pagar los saldos pendientes. Los estafadores también pueden utilizar tu número para recibir prestaciones médicas, por incapacidad y de otro tipo.

Robo de identidad médica

En el robo de identidad médica, alguien se hace pasar por otra persona para obtener atención médica gratuita.

Suplantación de identidad sintética

El robo de identidad sintética es un tipo de fraude en el que un **delincuente combina información real (normalmente robada) y falsa para crear una nueva identidad, que se utiliza para abrir cuentas fraudulentas y realizar compras fraudulentas.** El robo de identidad sintética permite al delincuente robar dinero a las compañías de tarjetas de crédito o a los prestamistas que conceden créditos basándose en la identidad falsa.

Robo de identidad de menores

En el robo de identidad de menores, alguien utiliza la identidad de un niño para obtener diversas formas de beneficio personal. Esto es habitual, ya que los niños no suelen tener asociada información que pueda suponer un obstáculo para el delincuente. El estafador puede utilizar el nombre y el número de la Seguridad Social del menor para obtener una residencia, encontrar empleo, obtener préstamos o evitar ser detenido por órdenes de detención pendientes. **A menudo, la víctima es un familiar, el hijo de un amigo u otra persona cercana al autor del delito**. Algunas personas incluso roban la información personal de seres queridos fallecidos.

Robo de identidad fiscal

El robo de identidad fiscal se produce cuando alguien utiliza tu información personal, incluido tu número de la Seguridad Social, para **presentar una declaración de la renta estatal o federal falsa en tu nombre y cobrar un reembolso.**

Robo de identidad

En el robo de identidad delictiva, **un delincuente se hace pasar por otra persona durante una detención** para intentar evitar una citación judicial, impedir que se descubra una orden de detención emitida a su nombre real o evitar un registro de detenciones o condenas.

Robo de identidad en el desempleo

Alguien utiliza tus datos personales para solicitar (y cobrar) prestaciones de desempleo.

- **Acoso sexual en Internet**

El acoso sexual en Internet se define como **una conducta sexual no deseada en cualquier plataforma digital y se reconoce como una forma de violencia sexual**. El acoso sexual en Internet abarca una amplia gama de comportamientos que utilizan contenidos digitales (imágenes, vídeos, mensajes, páginas) en una variedad de plataformas diferentes (privadas o públicas). Puede hacer que una persona se sienta amenazada, explotada, coaccionada, humillada, molesta, sexualizada o discriminada.

Tipos de acoso sexual en Internet

Intercambio no consentido de imágenes y vídeos íntimos

Imágenes y vídeos sexuales de una persona compartidos sin su consentimiento o tomados sin su consentimiento. Esto incluye una serie de comportamientos, como:

- Imágenes/vídeos sexuales tomados sin consentimiento ("creep shots" o "upskirting")
- Imágenes/vídeos sexuales tomados de forma consentida pero compartidos sin consentimiento ("porno de venganza")
- Actos sexuales no consentidos (por ejemplo, violación) grabados digitalmente (y potencialmente compartidos)

Explotación, coacción y amenazas

Una persona que recibe amenazas sexuales, es coaccionada para participar en comportamientos sexuales en línea o chantajeada con contenido sexual. Esto incluye una serie de comportamientos, como:

- Acosar o presionar a alguien en línea para que comparta imágenes sexuales de sí mismo o tenga un comportamiento sexual en línea (o fuera de ella).
- Utilizar la amenaza de publicar contenido sexual (imágenes, vídeos, rumores) para amenazar, coaccionar o chantajear a alguien ("sextorsión").
- Amenazas en Internet de naturaleza sexual (por ejemplo, amenazas de violación).
- Incitar a otros en Internet a cometer actos de violencia sexual.
- Incitar a alguien a participar en un comportamiento sexual y luego compartir pruebas de ello.

Acoso sexual

Una persona que es objeto y excluida sistemáticamente de un grupo o comunidad mediante el uso de contenidos sexuales que la humillan, molestan o discriminan. Esto incluye una serie de comportamientos, tales como:

- Cotilleos, rumores o mentiras sobre comportamientos sexuales publicados en línea, ya sea nombrando a alguien directamente o aludiendo indirectamente a alguien.
- Lenguaje sexual ofensivo o discriminatorio e insultos en línea
- Hacerse pasar por otra persona y dañar su reputación compartiendo contenidos sexuales o acosando sexualmente a otras personas.
- Compartir información personal en línea de forma no consentida para fomentar el acoso sexual ("doxing")
- Acoso por motivos de género u orientación sexual real o percibida
- La humillación corporal
- ‘Sacar a la luz’ a una persona anunciando públicamente en Internet su sexualidad o identidad de género sin su consentimiento.

Sexualización no deseada

Una persona que recibe solicitudes, comentarios y contenidos sexuales no deseados. Esto incluye una serie de comportamientos, como:

- Comentarios sexualizados (por ejemplo, en fotos)
- Campañas virales sexualizadas que presionan a la gente para que participe.
- Enviar a alguien contenido sexual (imágenes, emojis, mensajes) sin su consentimiento
- Insinuaciones sexuales inoportunas o petición de favores sexuales
- 'Bromas' de carácter sexual
- Calificar a los compañeros según su atractivo/actividad sexual
- Alterar imágenes de una persona para hacerlas sexuales

El acoso sexual de este tipo puede hacer que una persona sienta cualquiera de las siguientes cosas:

- Amenazado o asustado
- Explotado
- Coaccionado
- Que su dignidad es violada
- Humillados o degradados
- Avergonzado o juzgado
- Molesto
- Sexualizado
- Discriminados por su género u orientación sexual
- Sentirse culpable o tener la culpa

La experiencia y el impacto del acoso sexual en línea son únicos para cada persona y pueden sentirse tanto a corto plazo como a largo plazo en la salud mental y el bienestar. Los impactos a largo plazo pueden verse amplificados por la revictimización si el contenido se vuelve a compartir en línea, o porque el trauma inicial del incidente resurge mucho más tarde. Es importante reconocer que no hay una única manera en que un joven puede experimentar el acoso sexual en línea y que también puede afectar a otros que lo presencian.

- **Phishing**

Los ataques de phishing son **la práctica de enviar comunicaciones fraudulentas que parecen proceder de una fuente de confianza**. Suele realizarse a través del correo electrónico.

El objetivo es robar datos confidenciales, como información sobre tarjetas de crédito o datos de acceso, o instalar malware en la máquina de la víctima. El phishing es un tipo común de ciberataque que todo el mundo debería conocer para protegerse.

A veces, los hackers se conforman con obtener sus datos personales y la información de su tarjeta de crédito para obtener beneficios económicos. En otros casos, los correos electrónicos de phishing se envían para recopilar información de inicio de sesión de los empleados u otros detalles para utilizarlos en ataques más maliciosos contra unas pocas personas o una empresa concreta.

El phishing comienza con un correo electrónico fraudulento u otra comunicación diseñada para atraer a la víctima. El mensaje parece proceder de un remitente de confianza. Si se engaña a la víctima, se le induce a facilitar información confidencial, a menudo en un sitio web fraudulento. A veces también se descarga malware en el ordenador de la víctima.

Los ciberdelincuentes empiezan por identificar a un grupo de personas que quieren atacar. A continuación, **crean mensajes de correo electrónico y de texto que parecen legítimos, pero que en realidad contienen enlaces peligrosos, archivos adjuntos o señuelos que engañan a sus objetivos para que realicen una acción desconocida y arriesgada.**

Los riesgos de phishing incluyen:

- Robo de dinero de tu cuenta bancaria
- Cargos fraudulentos en tarjetas de crédito
- Pérdida de acceso a fotos, vídeos y archivos
- Publicaciones falsas en redes sociales realizadas en tus cuentas
- Ciberdelincuentes que suplantan su identidad ante un amigo o familiar, poniéndoles en peligro

En breve:

- **Los phishers suelen utilizar emociones como el miedo, la curiosidad, la urgencia y la codicia para obligar a los destinatarios a abrir archivos adjuntos o hacer clic en enlaces.**
- **Los ataques de phishing están diseñados para que parezcan proceder de empresas y particulares legítimos.**
- Los ciberdelincuentes innovan continuamente y se vuelven cada vez más sofisticados.
- Sólo se necesita un ataque de phishing para comprometer tu red y robar tus datos, por lo que **siempre es importante "pensar antes de hacer clic".**

Para evitar el phishing, CISCO (https://www.netacad.com/) da los siguientes consejos:

1. **Evite remitentes desconocidos**. Comprueba los nombres y las direcciones de correo electrónico antes de responder.
2. No te fíes de enlaces o archivos adjuntos en **correos electrónicos no solicitados**.
3. **Desconfía de los correos electrónicos marcados como "urgentes".**
4. Desconfía de los mensajes con **faltas de ortografía o gramática**.
5. **No se deje seducir por "ofertas"**. Suelen ser demasiado buenas para ser ciertas.
6. **Considera la posibilidad de utilizar un proveedor de correo electrónico seguro.**
7. **Nunca facilites información personal o financiera** basándote en una solicitud por correo electrónico.
8. Cuando reciba correos electrónicos de instituciones conocidas (gobierno, bancos, su médico), **vaya directamente a la fuente en lugar de hacer clic en los enlaces del correo electrónico**.
9. **Desconfíe de los saludos genéricos, como "Estimado señor o señora".**
10. Conozca **la política de tu proveedor de servicios para rastrear y detener el phishing**.
11. . No dé acceso a tu ordenador a un desconocido o a ayuda no solicitada.

- **Fraudes y estafas por Internet**

El fraude por Internet consiste en utilizar **servicios en línea y programas informáticos con acceso a Internet para estafar o aprovecharse de las víctimas**. El término "fraude por internet" abarca generalmente la actividad ciberdelictiva que tiene lugar a través de internet

o del correo electrónico, incluidos delitos como la usurpación de identidad, la suplantación de identidad y otras actividades de piratería informática diseñadas para estafar dinero.

Las estafas por Internet dirigidas a las víctimas a través de servicios en línea representan millones de dólares de actividad fraudulenta cada año, y las cifras siguen aumentando a medida que se extiende el uso de Internet y se sofistican las técnicas de los ciberdelincuentes.

Los ciberdelincuentes utilizan diversos vectores de ataque y estrategias para cometer fraudes en Internet. Esto incluye **software malicioso, servicios de correo electrónico y mensajería instantánea para propagar malware, sitios web falsos que roban datos de los usuarios y estafas de phishing elaboradas y de gran alcance**.

El fraude por Internet puede desglosarse en varios tipos de ataques clave, entre ellos:

Phishing (explicado en detalle más arriba): El uso del correo electrónico y los servicios de comunicación en línea para engañar a las víctimas y hacerles compartir datos personales, credenciales de acceso y detalles financieros.

Filtración de datos: Robo de datos confidenciales, protegidos o sensibles de una ubicación segura y su traslado a un entorno no fiable. Esto incluye el robo de datos de usuarios y organizaciones.

Denegación de servicio (DoS): Interrupción del acceso del tráfico a un servicio, sistema o red en línea con fines maliciosos.

Malware: El uso de software malicioso para dañar o inutilizar los dispositivos de los usuarios o robar datos personales y confidenciales.

Ransomware: Un tipo de malware que impide a los usuarios acceder a datos críticos y luego exige un pago con la promesa de restaurar el acceso. El ransomware suele distribuirse a través de ataques de phishing.

Correo electrónico comercial comprometido (BEC): Una forma sofisticada de ataque dirigido a empresas que realizan pagos por cable con frecuencia. Compromete cuentas de correo electrónico legítimas mediante técnicas de ingeniería social para enviar pagos no autorizados.

Algunos ejemplos:

- **Estafas con tarjetas de felicitación**

Muchos ataques fraudulentos por Internet se centran en acontecimientos populares para estafar a las personas que los celebran. Esto incluye cumpleaños, Navidad y Semana Santa, que suelen celebrarse compartiendo tarjetas de felicitación con amigos y familiares por correo electrónico. Los piratas informáticos suelen aprovecharse de ello instalando software malicioso dentro de una tarjeta de felicitación por correo electrónico, que se descarga e instala en el dispositivo del destinatario cuando abre la tarjeta de felicitación.

- **Estafas con tarjetas de crédito**

El fraude con tarjetas de crédito suele producirse cuando los piratas informáticos obtienen fraudulentamente los datos de las tarjetas de crédito o débito de las personas para intentar robar dinero o realizar compras. Para obtener estos datos, los estafadores de Internet suelen utilizar ofertas de tarjetas de crédito o préstamos bancarios demasiado buenas para ser ciertas para atraer a las víctimas. Por ejemplo, una víctima puede recibir un mensaje de su banco diciéndole que puede optar a un préstamo especial o que se ha puesto a su disposición una gran cantidad de dinero en forma de préstamo. Estas estafas siguen engañando a la gente a pesar de la conciencia generalizada de que tales ofertas son demasiado buenas para ser verdad por una razón.

- **Estafas en las citas por Internet**

Otro ejemplo típico de fraude por Internet es la gran cantidad de aplicaciones y sitios web de citas en línea. Los piratas informáticos se centran en estas aplicaciones para atraer a las víctimas y conseguir que envíen dinero y compartan datos personales con nuevos intereses amorosos. Los estafadores suelen crear perfiles falsos para interactuar con los usuarios, entablar una relación, ganarse poco a poco su confianza, crear una historia falsa y pedir ayuda económica al usuario.

- **Fraude en las tasas de lotería**

Otra forma común de fraude por Internet son las estafas por correo electrónico en las que se dice a las víctimas que han ganado la lotería. Estas estafas informan a los destinatarios de que sólo pueden reclamar su premio después de haber pagado una pequeña cantidad. Los

estafadores suelen elaborar los correos electrónicos de forma que parezcan y suenen creíbles, lo que hace que mucha gente caiga en el engaño. La estafa se centra en los sueños de la gente de ganar grandes cantidades de dinero, aunque nunca hayan comprado un billete de lotería. Además, ningún sistema de lotería legítimo pedirá a los ganadores que paguen para reclamar su premio.

- **El Príncipe de Nigeria**

La estafa del príncipe de Nigeria, una táctica clásica de fraude por Internet, sigue siendo común y próspera a pesar de la concienciación generalizada. La estafa utiliza la premisa de una familia o individuo nigeriano rico que quiere compartir su riqueza a cambio de ayuda para acceder a su herencia. Utiliza tácticas de suplantación de identidad para enviar mensajes de correo electrónico en los que se expone una historia emocional y, a continuación, atrae a las víctimas con la promesa de una importante recompensa económica. La estafa suele comenzar pidiendo una pequeña cantidad para ayudar con los trámites legales y el papeleo, con la promesa de una gran suma de dinero más adelante.

Inevitablemente, el estafador pedirá comisiones más elevadas para cubrir otras tareas administrativas y los costes de la transacción, respaldadas por documentos de confirmación de apariencia legítima. Sin embargo, la rentabilidad prometida nunca llega.

Consejos para evitar fraudes y estafas en Internet:

Es fundamental no enviar nunca dinero a alguien a quien se ha conocido por Internet, no compartir datos personales o financieros con personas que no sean legítimas o dignas de confianza, y no hacer clic en hipervínculos o archivos adjuntos de correos electrónicos o mensajes instantáneos. Una vez en el punto de mira, los internautas deben denunciar a las autoridades la actividad de los estafadores en línea y los correos electrónicos de phishing.

El fraude con tarjetas de crédito también puede evitarse vigilando de cerca las cuentas bancarias, estableciendo notificaciones sobre la actividad de las tarjetas de crédito, suscribiéndose a un servicio de supervisión del crédito y utilizando servicios de protección del consumidor. Si los usuarios sufren un fraude con tarjeta de crédito, deben denunciarlo a las autoridades legales competentes y a las agencias de crédito.

Spam

El spam es **cualquier tipo de comunicación digital no deseada y no solicitada que se envía en masa**. A menudo, el spam se envía por correo electrónico, pero también puede distribuirse a través de mensajes de texto, llamadas telefónicas o redes sociales.

Spam no es un acrónimo para una amenaza informática, aunque se han propuesto algunos (estúpido malware molesto sin sentido, por ejemplo). La inspiración para utilizar el término "spam" para describir los mensajes masivos no deseados es un sketch de los Monty Python en el que los actores declaran que todo el mundo debe comer el alimento Spam, lo quiera o no. Del mismo modo, todo el mundo con una dirección de correo electrónico debe, por desgracia, ser molestado por mensajes spam, nos guste o no.

Los spammers utilizan muchas formas de comunicación para enviar masivamente sus mensajes no deseados. Algunos son mensajes de marketing que venden productos no solicitados. Otros tipos de mensajes de spam pueden propagar programas maliciosos, engañarle para que divulgue información personal o asustarle haciéndole creer que tiene que pagar para salir del apuro.

Los filtros de spam del correo electrónico detectan muchos de estos tipos de mensajes, y las compañías telefónicas suelen advertir del "riesgo de spam" de las llamadas desconocidas. Ya sea por correo electrónico, mensaje de texto, teléfono o redes sociales, algunos mensajes de spam se cuelan, por lo que conviene saber reconocerlos y evitar estas amenazas. A continuación se indican varios tipos de spam a los que debe prestar atención:

- Correos electrónicos de phishing (ya descritos anteriormente)
- **Suplantación de identidad**. Los correos electrónicos falsos imitan un correo electrónico de un remitente legítimo y le piden que realice algún tipo de acción. Las falsificaciones bien ejecutadas contendrán marcas y contenidos familiares, a menudo de una gran empresa conocida como PayPal o Apple.
- **Estafas de soporte técnico**. En una estafa de soporte técnico, el mensaje de spam indica que tiene un problema técnico y que debe ponerse en contacto con el soporte técnico llamando al número de teléfono o haciendo clic en un enlace del mensaje.
- **Malspam**. Abreviatura de "spam con malware" o "spam malicioso", el malspam es un mensaje de spam que envía malware a su dispositivo. Los lectores desprevenidos que hacen clic en un enlace o abren un archivo adjunto acaban recibiendo algún tipo

de malware, como ransomware, troyanos, bots, ladrones de información, criptomineros, spyware y registradores de pulsaciones de teclas. Un método de entrega habitual consiste en incluir scripts maliciosos en un archivo adjunto de tipo familiar, como un documento de Word, un archivo PDF o una presentación de PowerPoint. Una vez abierto el archivo adjunto, los scripts se ejecutan y recuperan la carga maliciosa.

- **Llamadas y mensajes de spam**. ¿Ha recibido alguna vez una llamada robótica? Eso se llama spam. ¿Un mensaje de texto de un remitente desconocido instándole a hacer clic en un enlace desconocido? Eso se conoce como spam de mensajes de texto o "smishing", una combinación de SMS y phishing. Si recibes llamadas y mensajes de spam en tu Android o iPhone, la mayoría de las principales operadoras te dan la opción de denunciar el spam. Bloquear números es otra forma de combatir el spam móvil.

Hacking cibernético

Cualquiera que utilice un ordenador conectado a Internet es susceptible a las amenazas que plantean los piratas informáticos y los depredadores en línea. Estos villanos en línea suelen utilizar estafas de phishing, correo electrónico o mensajes instantáneos de spam y sitios web falsos para introducir malware peligroso en su ordenador y comprometer su seguridad informática.

Los piratas informáticos también pueden intentar acceder directamente a tu ordenador y a tu información privada si no está protegido por un cortafuegos. Pueden vigilar tus conversaciones o examinar el back-end de tu sitio web personal. Generalmente disfrazados con una identidad falsa, los depredadores pueden engañarte para que revele información personal y financiera sensible, o algo mucho peor.

Mientras tu ordenador está conectado a Internet, el malware que un pirata informático ha instalado en tu PC transmite silenciosamente tu información personal y financiera sin tu conocimiento ni consentimiento. O bien, un depredador informático puede abalanzarse sobre la información privada que usted ha revelado sin darse cuenta. En cualquiera de los casos, podrán:

- Secuestrar tus nombres de usuario y contraseñas
- Robar tu dinero y abrir tarjetas de crédito y cuentas bancarias a tu nombre

- Arruinar tu crédito
- Solicitar nuevos números de identificación personal (PIN) o tarjetas de crédito adicionales
- Realizar compras
- Añadirse a sí mismos o a un alias que controlen como usuario autorizado para que sea más fácil utilizar tu crédito
- Obtener anticipos en efectivo
- Usar y abusar de tu número de la Seguridad Social
- Vender tu información a terceros que la utilizarán con fines ilícitos o ilegales

Para protegerte de estas amenazas, puedes hacer lo siguiente:

1. **Comprobar continuamente la exactitud de las cuentas personales y tratar de inmediato cualquier discrepancia.**
2. **Extrema las precauciones** cuando entres en salas de chat o publiques páginas web personales.
3. **Limite la información personal** que publicas en tus páginas web personales.
4. Vigilar atentamente las solicitudes de "amigos" o conocidos en línea para detectar conductas depredadoras.
5. **Mantenga la información personal y financiera fuera de las conversaciones en línea.**
6. **Extreme las precauciones cuando acepte reunirse en persona con un "amigo"** o conocido en línea.
7. **Utilice un cortafuegos bidireccional.**
8. **Actualice regularmente tu sistema operativo.**
9. **Aumente la configuración de seguridad de su navegador.**
10. **Evite los sitios web dudosos**
11. **Descargue software sólo de sitios en los que confíe**. Evalúa cuidadosamente el software gratuito y las aplicaciones de intercambio de archivos antes de descargarlos.
12. **No abras mensajes de remitentes desconocidos.**
13. **Borra inmediatamente los mensajes que sospeches que son spam.**
14. **Asegúrate de tener instalados en tu PC los mejores productos de software de seguridad:** Utilice protección antivirus y obtenga protección antispyware.

Cyber stalking

El cyberstalking se refiere al **uso de Internet y otras tecnologías para acosar o acechar a otra persona en línea.**

Este acoso en línea, que es una extensión del ciberacoso y del acoso en persona, puede adoptar la forma de correos electrónicos, mensajes de texto, publicaciones en redes sociales, etc., y suele ser metódico, deliberado y persistente. La mayoría de las veces, las interacciones no terminan, aunque el destinatario exprese su desagrado o pida a la persona que se detenga. **El contenido dirigido al objetivo suele ser inapropiado y a veces incluso perturbador, lo que puede hacer que la persona se sienta temerosa, angustiada, ansiosa y preocupada.**

Cuando se trata de cyberstalking, los que se dedican a este comportamiento utilizan una variedad de tácticas y técnicas para acosar, humillar, intimidar y controlar a sus objetivos. De hecho, muchos de los que se dedican al cyberstalking son expertos en tecnología, además de creativos, e idean multitud de formas de atormentar y acosar a sus objetivos. He aquí algunos ejemplos de lo que pueden hacer quienes se dedican al cyberstalking:

- **Publicar comentarios groseros, ofensivos o sugerentes en Internet.**
- **Seguir a la víctima en Internet** uniéndose a los mismos grupos y foros**.**
- **Enviar mensajes o correos electrónicos amenazadores, controladores o lascivos** a la víctima.
- Utilizar la tecnología para amenazar o chantajear a la víctima.
- **Etiquetar excesivamente a la víctima**, aunque no tenga nada que ver con ella.
- Comentar o dar "me gusta" a todo lo que la víctima publique en Internet.
- **Crear cuentas falsas para seguir a la víctima** en las redes sociales.
- Enviar mensajes al objetivo repetidamente.
- **Hackear o secuestrar las cuentas en línea de la víctima.**
- Intentar extorsionar con sexo o fotos explícitas.
- Enviar regalos u objetos no deseados a la víctima.
- **Difundir información confidencial en línea.**
- Publicar o distribuir fotos reales o falsas de la víctima.
- **Bombardear a la víctima con fotos suyas sexualmente explícitas.**
- Crear mensajes falsos para avergonzar a la víctima.

- Rastrear los movimientos en línea de la víctima instalando dispositivos de seguimiento.
- **Hackear la cámara del portátil o smartphone de la víctima para grabarla en secreto.**
- Continuar con el comportamiento acosador incluso después de pedirles que cesen.

Al igual que el stalking, el cyberstalking puede tener consecuencias físicas y emocionales muy diversas para quienes lo sufren. Por ejemplo, no es infrecuente que quienes sufren acoso en línea experimenten ira, miedo y confusión. También pueden tener problemas para dormir e incluso quejarse de problemas de estómago.

Las formas de prevenir el cyberstalking son muy similares a las recomendadas para prevenir otras ciberamenazas, ya que todas ellas están conectadas y funcionan de forma parecida. Algunos de los consejos son:

- **Crea contraseñas seguras**. Asegúrate de tener contraseñas seguras para todas tus cuentas en Internet, así como contraseñas seguras para tus dispositivos. A continuación, configura un recordatorio en tu teléfono para cambiar regularmente tus contraseñas. **Elige contraseñas que sean difíciles de adivinar pero fáciles de recordar.**
- **Asegúrate de cerrar sesión cada vez**. Puede parecer una molestia, pero asegúrate de cerrar la sesión de correo electrónico, cuentas de redes sociales y otras cuentas en línea después de utilizarlas. De este modo, si alguien consiguiera entrar en tu dispositivo, no tendría fácil acceso a tus cuentas.
- **No pierdas de vista tus dispositivos. No dejes el teléfono sobre la mesa del trabajo ni te alejes de un portátil abierto.** Sólo hacen falta uno o dos minutos para que alguien instale un dispositivo de rastreo o piratee tu dispositivo. Por lo tanto, asegúrate de tener estos objetos en tu poder o de asegurarlos de alguna manera.
- **Ten cuidado con el wifi público**. Reconoce el hecho de que si utilizas wifi público en hoteles o en la cafetería local, te estás poniendo en riesgo de ser hackeado. Trate de abstenerse de usar wifi público o invierta en VPN.
- **Practique hábitos de seguridad en línea**. En otras palabras, prioriza aceptar solicitudes de amistad sólo de personas que conozcas y mantén la privacidad de tus publicaciones. También deberías plantearte tener una dirección de correo electrónico específica para tu actividad en Internet. Utilice este correo electrónico cuando haga sus compras en línea o se inscriba en programas de fidelización.

- **Aproveche la configuración de seguridad.** Revise cada una de sus cuentas en Internet -especialmente sus cuentas en redes sociales- y asegúrese de que utiliza la configuración de privacidad más estricta posible. Incluso puedes establecer una configuración que impida que te etiqueten o publiquen fotos tuyas sin tu aprobación previa.
- **Crea nombres de usuario genéricos.** En lugar de utilizar tu nombre completo en Internet, considera la posibilidad de crear un nombre de usuario o seudónimo de género neutro. De este modo, dificultarás que te encuentren. También deberías dejar en blanco las secciones opcionales, como tu fecha de nacimiento o tu ciudad de origen.
- **Mantén las ubicaciones seguras.** Considera la posibilidad de desactivar la configuración de geolocalización en las fotos. También deberías abstenerte de publicar tu ubicación en tiempo real y, en su lugar, publicar fotos que muestren dónde has estado después del hecho.

- **Tenga cuidado con los sitios de citas en línea.** Absténgase de utilizar su nombre completo en los sitios de citas en línea. También debes evitar dar información personal como tu apellido, dirección, correo electrónico y número de teléfono hasta que os hayáis conocido en persona y hayáis establecido un nivel de confianza.

- **Realiza una auditoría de las redes sociales**. Siempre es una buena idea revisar tus cuentas en las redes sociales y eliminar las fotos o publicaciones que proporcionen demasiada información sobre ti o que creen una imagen que no quieres que se difunda. Ten en cuenta también que, aunque hayas bloqueado a alguien en las redes sociales, puede seguir viendo tu cuenta utilizando la de otra persona o creando un perfil falso.

Las formas de hacer frente al cyberstalking, en caso de que ya se esté produciendo, incluyen:

- **Dile a la persona que deje de hacerlo.** Responde una sola vez a la persona que te acosa cibernéticamente y dile que deje de ponerse en contacto contigo. No hace falta que digas nada en concreto ni que expliques tu respuesta, simplemente pídele que no vuelva a ponerse en contacto contigo.

- **Bloquea a la persona.** Asegúrate de bloquear a la persona que te acosa cibernéticamente de todas tus cuentas. Debes bloquearla en las redes sociales y en tu smartphone.
- **Niégate a responder a cualquier contacto**. Si la persona que te acosa cibernéticamente sigue buscando formas de ponerse en contacto contigo, no respondas a nada de lo que publique o te envíe.
- **Cambia de dirección de correo electrónico y de nombre de usuario**. Considera la posibilidad de cambiar de dirección de correo electrónico y de nombre de usuario para dificultar que la persona que te acosa cibernéticamente se ponga en contacto contigo.

Si has pedido a la persona que te acosa cibernéticamente que deje de hacerlo y su comportamiento continúa, es importante tomar medidas contra ella. Esto incluye ponerse en contacto con las autoridades competentes y reunir pruebas de sus actos. También puede considerar la posibilidad de hablar con un abogado. **Estos son los puntos clave que habrá que tener en cuenta a la hora de tomar medidas.** La policía local puede informarle de si hay algo más que pueda hacer para mantenerse a salvo.

- **Guarda pruebas de todo**. Aunque tengas ganas de destruirlo todo, es importante que guardes copias de todo lo que te haya enviado la persona que te acosa cibernéticamente. Haz una copia para ti y otra para la policía.
- **Avisa a la policía local**. Es importante avisar a la policía y presentar una denuncia oficial si te están acosando cibernéticamente. Aunque no puedan hacer nada de inmediato, tener una denuncia oficial archivada es importante si el comportamiento persiste o se intensifica.
- **Denúncialo ante el sitio o servicio que haya utilizado**. Si la persona que te acosa cibernéticamente te ha acosado a través de Facebook, Instagram, Twitter, Snapchat, YouTube, Gmail o algún otro método, informa a las autoridades competentes de lo que estás sufriendo. Muchas veces, estas organizaciones se toman en serio las denuncias de cyberstalking y se ocuparán del asunto.

3.3. Cómo denunciar las amenazas a la ciberseguridad en las redes sociales/instituciones

Todas las redes sociales han establecido mecanismos para denunciar distintos tipos de amenazas a la ciberseguridad, como la incitación al odio en línea, la usurpación de identidad, el acoso sexual, el ciberacoso, etc. A continuación, encontrará información sobre algunas de las redes sociales más populares:

- **Facebook**

Los problemas de seguridad en Facebook tienen múltiples categorías. Puede que haya un contenido abusivo o una página de odio que quieras denunciar o puede que alguien esté suplantando tu identidad en Facebook, etc. La mejor forma de denunciar contenido abusivo o spam en Facebook es utilizando el enlace Denunciar que hay cerca del propio contenido.

Para denunciar un perfil:

1. Vaya al perfil que quieres denunciar haciendo clic en su nombre en tu Feed o buscándolo.
2. Haz clic en "..." a la derecha y selecciona Buscar soporte o denunciar perfil.
3. Para dar tu opinión, haz clic en la opción que mejor describa cómo este perfil va en contra de sus Normas comunitarias y, a continuación, haz clic en Siguiente.
4. En función de tus comentarios, es posible que puedas enviar un informe a Meta. Para algunos tipos de contenido, Facebook no te pide que envíes un informe, pero utiliza tus comentarios para ayudar a sus sistemas a aprender.
5. Haz clic en Listo.

Para denunciar un post:

1. Vaya al mensaje que desea denunciar.
2. Haz clic en "..." en la parte superior derecha de la entrada.
3. Haz clic en Buscar soporte o Denunciar publicación.
4. Para dar tu opinión, haz clic en la opción que mejor describa cómo esta publicación va en contra de las Normas comunitarias de Facebook. Haz clic en Siguiente.

5. En base a tus comentarios, es posible que puedas enviar un informe a Meta. Para algunos tipos de contenido, Facebook no te pide que envíes un informe, pero utiliza tus comentarios para ayudar a sus sistemas a aprender.
6. Haz clic en Listo.

Para denunciar una foto o un vídeo:

1. Haz clic en la foto o el vídeo para ampliarlo. Si el perfil está bloqueado y no puedes ver la foto a tamaño completo, haz clic en Buscar soporte o Denunciar foto.
2. Haz clic en "..." a la derecha de la foto o el vídeo.
3. Haz clic en Buscar soporte o Denunciar foto para las fotos o en Denunciar vídeo para los vídeos.
4. Selecciona la opción que mejor describa el problema y sigue las instrucciones en pantalla.

Para denunciar un mensaje contrario a las Normas comunitarias de Facebook:

1. Desde cualquier página de Facebook, haz clic en el icono de Messenger de la parte superior derecha.
2. Abre el mensaje.
3. Si abriste el mensaje como una ventana emergente, haz clic en el icono de configuración.
4. Haga clic en Algo va mal.
5. Para dar tu opinión, haz clic en la opción que mejor describa cómo este mensaje va en contra de las Normas comunitarias de Facebook.
6. En función de tus comentarios, es posible que puedas enviar un informe a Meta. Para algunos tipos de contenido, Facebook no te pide que envíes un informe, pero utiliza tus comentarios para ayudar a sus sistemas a aprender.

Para denunciar una página:

1. Vaya a la página que quieres denunciar haciendo clic en su nombre en tu Feed o buscándola.
2. Haz clic en más debajo de la foto de portada de la página.
3. Selecciona Buscar soporte o Denunciar página.
4. Para dar tu opinión, haz clic en la opción que mejor describa cómo esta página va en contra de las Normas comunitarias de Facebook.

5. En función de tus comentarios, es posible que puedas enviar un informe a Meta. Para algunos tipos de contenido, Facebook no te pide que envíes un informe, pero utiliza tus comentarios para ayudar a sus sistemas a aprender.

Para denunciar a un grupo:

1. Vaya al grupo que quieres denunciar haciendo clic en su nombre en tu Feed o buscándolo.
2. Haz clic en más debajo de la foto de portada del grupo.
3. Selecciona Denunciar grupo.

Para denunciar un evento:

1. Desde tu Feed, haga clic en Eventos en el menú de la izquierda.
2. Vaya al evento del que desea informar.
3. Haz clic en "..." y selecciona 'Informar de evento'.
4. Para dar tu opinión, haz clic en la opción que mejor describa cómo este perfil va en contra de las Normas comunitarias de Facebook.
5. En función de tus comentarios, es posible que puedas enviar un informe a Meta. Para algunos tipos de contenido, Facebook no te pide que envíes un informe, pero utiliza tus comentarios para ayudar a sus sistemas a aprender.

Para denunciar un comentario:

1. Vaya al comentario que desea denunciar.
2. Haz clic en "..." junto al comentario.
3. Haz clic en Dar opinión o Denunciar este comentario.
4. Para opinar, haz clic en la opción que mejor describa cómo este comentario va en contra de las Normas comunitarias de Facebook. Si no ves ninguna opción que se ajuste, haz clic en Otra cosa para buscar más.
5. En función de tus comentarios, es posible que puedas enviar un informe a Meta. Para algunos tipos de contenido, Facebook no te pide que envíes un informe, pero utiliza tus comentarios para ayudar a sus sistemas a aprender.

Para denunciar un anuncio en Facebook:

1. Vaya al anuncio que desea denunciar haciendo clic en su nombre en su Feed o buscándolo.

2. Haga clic en "..." junto al anuncio que desea denunciar.
3. Haga clic en Denunciar anuncio y siga las instrucciones que aparecen en pantalla

- **Instagram**

Denunciar los posts:

Si ves una publicación, un mensaje o una cuenta que crees que infringe las Normas de la comunidad de Instagram, puedes denunciarlo. Puedes denunciar contenidos individuales tocando los tres puntos sobre una publicación, manteniendo pulsado un mensaje o visitando una cuenta y denunciando directamente desde el perfil. Para más información, visita el Centro de ayuda de Instagram https://help.instagram.com/

Denunciar las cuentas

Las cuentas que infrinjan las Normas de la comunidad de Instagram pueden denunciarse en la aplicación o a través de un formulario web. Para obtener más información, consulta el Centro de ayuda

Denunciar los comentarios:

1. Si ves un comentario que es spam o que pretende intimidarte o acosarte a ti o a otra persona, denúncialo.
2. Abre la conversación en la app de Instagram.
3. Mantén pulsado el mensaje individual que quieras denunciar.
4. Pulsa Informar.
5. Seleccione una razón por la que está informando del mensaje y, a continuación, pulse enviar informe.
6. Para obtener más información, visite el Centro de ayuda.

Denunciar mensajes

Si recibes un mensaje que te parece inapropiado, mantén pulsado el mensaje individual para denunciarlo. Para obtener más información, visite el Centro de ayuda.

Denunciar historias

1. Si ves la historia de alguien y crees que va en contra de las Normas de la Comunidad de Instagram, puedes denunciarla.
2. Abre la historia.
3. Toca los 3 puntos de la parte inferior de la foto o el vídeo que quieras denunciar.
4. Toca Denunciar y, a continuación, sigue las instrucciones que aparecen en pantalla.

5. Para obtener más información, visite el Centro de ayuda

- **TikTok**

Para preguntas, dudas o problemas con tu perfil, puedes encontrar información y apoyo en el Centro de Ayuda de TikTok (https://support.tiktok.com/en/). En la sección 'Seguridad', puedes ir a 'Reportar un problema' y reportar un video en VIVO, un comentario en VIVO, un video, un comentario, un mensaje directo, un sonido, un hashtag, y también puedes reportar a alguien. Los pasos son muy fáciles de seguir, sólo tienes que encontrar la opción Denunciar y seguir las instrucciones.

Para preguntas, dudas o problemas con la política de privacidad o fraude de TikTok, puedes encontrar soporte en este enlace https://privacytiktok.zendesk.com/hc/en-us/requests/new . Serás redirigido a un formulario online donde podrás solicitar información sobre tus datos, denunciar una violación de privacidad o preguntar sobre un problema de privacidad en particular.

- **Twitter**

En el Centro de Ayuda de Twitter (https://help.twitter.com/en/safety-and-security) puedes encontrar información y ayuda en caso de cuentas comprometidas y pirateadas, sobre privacidad, spam y cuentas falsas, contenido sensible y ofensivo, comportamiento abusivo y su denuncia.

Para denunciar un Tweet:

1. Navega hasta el Tweet que deseas denunciar en twitter.com o desde la aplicación Twitter para iOS o Twitter para Android.
2. Selecciona el icono "...".
3. Selecciona Denunciar.
4. Seleccione para quién es el informe: Yo mismo, Otra persona o un grupo específico de personas, o Todos en Twitter.
5. A continuación, Twitter te pedirá que proporciones más información sobre el problema que estás denunciando. Twitter también puede pedirte que selecciones Tweets adicionales de la cuenta que estás denunciando para tener un mejor contexto para evaluar tu denuncia.

6. Twitter se asegurará de que tiene tu información correcta confirmando lo que estás denunciando, así como el contexto adicional que has compartido, y qué norma puede haber infringido.
7. Twitter incluirá el texto de los Tweets denunciados en los correos electrónicos y notificaciones de seguimiento que te envíe. Para optar por no recibir esta información, puedes desmarcar la casilla junto a Actualizaciones sobre este informe que puede mostrar estos Tweets.
8. Una vez que hayas enviado tu informe, Twitter te proporcionará recomendaciones sobre acciones adicionales que puedes llevar a cabo para mejorar tu experiencia en Twitter.

Para denunciar una cuenta:

1. Vaya al perfil de la cuenta y seleccione el icono "...".
2. Seleccione Denunciar.
3. Seleccione para quién es el informe: Yo mismo, Otra persona o un grupo específico de personas, o Todos en Twitter.
4. A continuación, Twitter te pedirá que proporciones información adicional sobre el problema que estás denunciando. También pueden pedirte que selecciones Tweets de esa cuenta para tener un mejor contexto para evaluar tu informe.
5. Twitter se asegurará de que tienen tu información correcta confirmando lo que estás denunciando, así como el contexto adicional que has compartido y qué norma puede haber infringido.
6. Twitter incluirá el texto de los Tweets que has denunciado en los correos electrónicos y notificaciones de seguimiento que te envíe. Para optar por no recibir esta información, puedes desmarcar la casilla junto a Actualizaciones sobre este informe que puede mostrar estos Tweets.
7. Una vez que hayas enviado tu informe, Twitter te proporcionará recomendaciones sobre acciones adicionales que puedes llevar a cabo para mejorar tu experiencia en Twitter.

Para denunciar un mensaje individual o una conversación:

1. Selecciona la conversación de Mensajes Directos y busca el mensaje que deseas denunciar. (Para denunciar toda la conversación, haz clic en el icono "...").
2. Selecciona el icono "i" de información y selecciona Denunciar @nombredeusuario.

3. Si seleccionas Es abusivo o dañino, Twitter te pedirá que proporciones información adicional sobre el problema que estás denunciando. También pueden pedirte que selecciones mensajes adicionales de la cuenta que estás denunciando para tener un mejor contexto para evaluar tu denuncia.
4. Una vez que hayas enviado tu informe, Twitter te proporcionará recomendaciones sobre acciones adicionales que puedes llevar a cabo para mejorar tu experiencia en Twitter.

- **¿Cuándo se considera un delito?**

España

En España, **las consecuencias de los delitos contra la ciberseguridad van desde cinco años de cárcel hasta multas de hasta 2.700 euros.**

El stalking se convierte en delito cuando alguien restringe repetidamente la sensación de seguridad de una persona y cuando hace que la víctima se sienta humillada, insultada, amenazada. Como es lógico, quien lo practique tiene que enfrentarse a varias consecuencias que van de tres meses a dos años de prisión o el pago de una multa a la víctima, una cantidad diaria de dinero que deciden los jueces. Una multa diaria de 15 euros durante seis meses asciende a un total de 2.700 euros.

La revelación de secretos también tiene consecuencias en España, ya que es un delito grave. Cualquier persona que "*sin autorización del afectado, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales*" puede enfrentarse también a penas de prisión o al pago de multas. **La difusión de imágenes de contenido sexual** es aún más grave y puede tener consecuencias adicionales.

Además, es necesario hablar del **robo de identidad**. Se trata de la apropiación de la identidad de una persona. En otras palabras, hacerse pasar por esa persona, asumiendo su identidad ante otros. Un ejemplo podría ser la creación de una cuenta en una red social intentando suplantar la identidad de otra persona para recabar información o para cualquier otro fin. Se castiga con penas de prisión de seis meses a tres años.

Hay que poner freno a estas amenazas a la ciberseguridad. Por ello, en España existe una forma de llevarlo a un plano legal. En primer lugar, **cualquier víctima que quiera tomar medidas debe, en primer lugar, recopilar pruebas de lo que está ocurriendo y denunciarlo en comisaría lo antes posible**. Tras hacerlo se pondrán en contacto contigo después de

haberlo comprobado y valorarán la situación. Si lo encuentran conveniente, la denuncia iniciará un nuevo proceso y se emprenderán acciones legales.

Bélgica

La ciberseguridad es el resultado de un conjunto de medidas de seguridad que minimizan el riesgo de interrupción o acceso no autorizado a los sistemas de información y comunicación (TIC). Incluye todas las medidas razonables y aceptables para proteger las TIC de los ciudadanos, las empresas, las organizaciones y el gobierno frente a las ciberamenazas. La ciberseguridad implica proteger los sistemas (como el hardware, el software y la infraestructura relacionada) y las redes, así como los datos que contienen.

La Evaluación Nacional de Riesgos de Bélgica 2018-2023 del Centro Nacional de Crisis considera la ciberseguridad como uno de los principales riesgos a los que se enfrentará Bélgica en los próximos años. Dentro de este grupo, **la ciberdelincuencia y el hacktivismo** se identifican como riesgos nacionales prioritarios.

Esta definición procede del "Centro para la Ciberseguridad en Bélgica", la autoridad nacional para la ciberseguridad en Bélgica, que también especifica las 4 amenazas principales a las que pretende responder la ciberseguridad: servicios militares y de inteligencia extranjeros, terrorismo, hacktivismo y ciberdelincuencia. En este informe, la ciberseguridad en la que nos centraremos estará principalmente relacionada con el hacktivismo y la ciberdelincuencia debido a sus métodos de ataque más utilizados, las redes sociales, y debido al impacto directo que tienen en la seguridad general de todos los ciudadanos, incluidos los jóvenes.

En julio de 2016, se adoptó la Directiva sobre la seguridad de las redes y los sistemas de información (Directiva SRI) (https://www.itgovernance.eu/nl-be/nis-directive-be), que se transpuso a la legislación belga el 7 de abril de 2019: Ley por la que se establece un marco para la seguridad de las redes y los sistemas de información de interés público para la seguridad pública. El artículo 7 de esta Directiva (reproducido en el artículo 10 de la Ley NIS belga) exige a los Estados miembros que elaboren una estrategia nacional para la seguridad de los sistemas de red y de información. Hasta la publicación de la Ley belga sobre redes y sistemas de información (NIS) en mayo de 2019, el país no contaba con una legislación completa sobre ciberseguridad.

Este gran paso se ha conseguido gracias a la Agencia de Ciberseguridad de la Unión Europea (ENISA) que contribuye a la ciberpolítica de la UE, mejora la fiabilidad de los productos,

servicios y procesos TIC con sistemas de certificación de ciberseguridad, coopera con los Estados miembros y los organismos de la UE y ayuda a Europa a prepararse para los retos cibernéticos del mañana. Además, cabe destacar la siguiente legislación que se utilizará en función de la ciberdelincuencia que se persiga:

- Código Penal belga: art. 550 (b) "Hacking", art. 210bis "Fraude informático".
- Ley de 1 de julio de 2011 sobre seguridad y protección de infraestructuras críticas.
- Directiva (UE) 2016/1148, de 6 de julio de 2016, relativa a medidas para un elevado nivel común de seguridad de las redes y sistemas de información en toda la Unión.
- Ley de 7 de abril de 2019, por la que se establece un marco para la red de seguridad y los sistemas de información de interés general para la seguridad pública.
- Real Decreto de 12 de julio de 2019, por el que se desarrolla la Ley de 7 de abril de 2019, por la que se establece el marco para la red de seguridad y los sistemas de información de interés general para la seguridad pública.
- Reglamento (UE) 2019/881, de 17 de abril de 2019, relativo a la ENISA.
- Reglamento de Ejecución (UE)2018/151 de la Comisión, de 30 de enero de 2018, por el que se establecen disposiciones de aplicación de la Directiva UE 2016/1148 del Parlamento Europeo y del Consejo en lo que respecta a una mayor especificación de los elementos que deben tener en cuenta los proveedores de servicios digitales para gestionar los riesgos de seguridad.

Países Bajos

En 2021, casi 2,5 millones de neerlandeses mayores de 15 años declararon haber sido víctimas de la ciberdelincuencia, lo que representa casi el 17% de la población.

El Parlamento neerlandés ha promulgado legislación sobre ciberdelincuencia que impide lo siguiente:

- Artículo 138a: Toda persona que El que intencionada e ilícitamente acceda a un sistema automatizado de almacenamiento o tratamiento de datos, o a una parte de dicho sistema.
- Artículo 138b: la obstaculización grave e ilícita del tratamiento de datos.
- Artículo 232: la falsificación de cualquier ficha electrónica que tenga valor probatorio y el uso de dichas fichas como si fueran auténticas.

La ciberdelincuencia se define como *"los delitos que implican formas digitales de usurpación de identidad, fraude al comprar o vender en línea, piratería informática y acoso cibernético (calumnias, stalking, chantaje y amenazas de violencia cometidas en línea)*.'[26]

Cybercrimes relating to individual, organisational and governmental privacy are criminalised under Dutch law (in accordance with the articles above). Common cybercrimes reported in the Netherlands are **Hacking**, **Online shopping fraud** and **Cyber bullying**

Los ciberdelitos relacionados con la privacidad individual, organizativa y gubernamental están tipificados como delito en la legislación neerlandesa (de conformidad con los artículos anteriores). Los ciberdelitos más comunes en los Países Bajos son el pirateo informático**, el fraude en las compras en línea y el ciberacoso**[27]. Los ciberdelitos más comunes, identificados por el Gobierno neerlandés, son los siguientes [28]:

- Phishing: uso de mensajes de correo electrónico falsos para obtener información personal de los internautas.
- Uso indebido de información personal ("robo de identidad").
- Piratería informática: cierre o uso indebido de sitios web o redes informáticas.
- Difusión del odio e incitación al terrorismo.
- Distribuir pornografía infantil.
- Grooming: hacer insinuaciones sexuales a menores.

La Seguridad Cibernética Nacional (NCSC) (https://english.ncsc.nl/) es responsable de supervisar la seguridad digital en los Países Bajos[29]. Para ello Supervisa continuamente todas las fuentes sospechosas en Internet, asesora a las organizaciones sobre cómo protegerse de las amenazas en línea y supervisa la evolución de la tecnología digital y la actualización de los sistemas de seguridad.

Bulgaria

Por "ciberdelincuencia" (también denominada "delincuencia informática" o "delincuencia de alta tecnología") debe entenderse "*los actos delictivos cometidos mediante el uso de redes de comunicación y sistemas de información electrónicos, o contra dichas redes y sistemas*".

[26] The Netherlands in Numbers : https://longreads.cbs.nl/the-netherlands-in-numbers-2020/what-about-cyber-crime/#:~:text=Hacking%2C%20online%20shopping%20fraud%20and%20cyber%20bullying&text=Hacking%20was%20most%20common%2C%20mentioned,such%20as%20stalking%20or%20threats.
[27] Ibid
[28] Forms of Cybercrime: https://www.government.nl/topics/cybercrime/forms-of-cybercrime
[29] Fighting Cybercrime in the Netherlands: https://www.government.nl/topics/cybercrime/fighting-cybercrime-in-the-netherlands

De hecho, el término se refiere a tres categorías de actos delictivos. La primera abarca tipos tradicionales de delitos como el fraude o la falsificación, aunque en el contexto de la ciberdelincuencia esta categoría se refiere en particular a los delitos cometidos a través de redes de comunicación y sistemas de información electrónicos ("redes electrónicas"). La segunda se refiere a la publicación en medios electrónicos de contenidos ilegales (como pornografía infantil o contenidos que incitan a la violencia y están relacionados con la incitación al odio y la discriminación). El tercero incluye delitos específicos de las redes electrónicas, como los ataques contra los sistemas de información, la denegación de servicio y la piratería informática.

Bulgaria ha ratificado el Convenio sobre la Ciberdelincuencia, adoptado por el Consejo de Europa en 2001, y sus protocolos. Sobre esta base, el Código Penal de Bulgaria incluye definiciones y sanciones relacionadas con los ciberdelitos. El Código Penal describe diferentes tipos de ciberdelitos:

- El fraude cibernético se define en el Art. 212a
- Una forma especial de destrucción y daño mediante herramientas digitales se define en el Art. 216, apartado 2
- En el art. 171 se define una forma específica de violación del secreto de la correspondencia. 171.
- También se tipifica específicamente la pornografía infantil.
- Los ciberdelitos recogidos en el Capítulo 9 del Código Penal (Art. 319a a Art. 319f del Código Penal). Afectan a las relaciones públicas que garantizan el buen funcionamiento de los ordenadores, los sistemas informáticos, los recursos informáticos y las redes informáticas, así como la creación y utilización lícitas de la información. Incluyen el acceso no autorizado, la alteración, el daño, la destrucción de datos o programas, la introducción de un virus o la difusión de contraseñas.
- El primero se refiere a la copia o utilización de datos informáticos sin permiso mediante el acceso no autorizado a recursos informáticos (artículo 319a).
- El siguiente tipo de delito informático es la falsificación o destrucción de un programa o datos informáticos (artículo 319b). Esto incluye la adición, modificación o supresión de un programa informático o de datos informáticos, haciéndolos inauténticos o incoherentes con los programas y datos originales.

- La introducción de un virus informático en un ordenador o red de información se contempla en el Art. 319d, párrafo 1 del Código Penal.
- El Artículo 319e, párrafo 1 del Código Penal, incluye la distribución de contraseñas de ordenadores o sistemas, cuando ello conlleve la revelación de datos o secretos personales. La pena es de hasta un año de prisión.

En términos de privacidad y seguridad en línea, es importante mencionar que la normativa búlgara está relacionada con el GDPR, regulado por la Comisión de Protección de Datos Personales (https://www.cpdp.bg/). Se trata de un organismo estatal independiente que protege a las personas en el tratamiento de sus datos personales y en el acceso a los mismos, así como en el control del cumplimiento de la Ley de Protección de Datos Personales. Es un órgano colegiado independiente y está compuesto por un presidente y cuatro miembros. Los miembros de la comisión y su presidente son elegidos por la Asamblea Nacional a propuesta del Consejo de Ministros por un mandato de 5 años y pueden ser reelegidos para otro mandato. Una de las funciones más importantes de la Comisión es remitir al Tribunal de Justicia de Bulgaria los asuntos relacionados con la infracción del RGPD.

3.4. Cómo evitar los riesgos de seguridad de los datos

Una de las cosas más importantes para mantener nuestros datos protegidos es tener una contraseña segura. Será muy útil, ya que hoy en día los ciberdelincuentes no paran de idear nuevas e innovadoras formas de piratear cuentas y hacerse con datos personales. Algunas consecuencias potenciales de las contraseñas débiles son la violación de datos, el robo de identidad, el secuestro informático, el chantaje y la pérdida de privacidad.

Por lo tanto, para evitar que la gente sufra estas consecuencias, aquí tienes instrucciones sobre cómo crear una contraseña segura en la que puedas confiar.

- **Nunca utilices información personal**. Puede parecer obvio, pero mucha gente utiliza su propia información personal al crear su contraseña. Se recomienda no utilizar nombres, cumpleaños, direcciones o números de teléfono.
- **Incluye una combinación de letras, números y símbolos**. Cuantos más caracteres aleatorios utilices, más compleja será tu contraseña.
- **Prioriza la longitud de la contraseña**. Disminuirá las posibilidades de ser víctima de un ciberataque.

- **No repita nunca las contraseñas**. La gente está acostumbrada a elegir siempre la misma contraseña. Esto es un gran error ya que los pone en riesgo de ataques de relleno de credenciales.
- **Evite utilizar palabras reales**. Los hackers utilizan programas maliciosos que pueden procesar cada palabra encontrada en un diccionario para descifrar contraseñas. Por lo tanto, utilizar palabras inventadas puede ayudar a crear una contraseña fuerte y segura.

Además, para mantener su información protegida se recomienda **utilizar sólo sitios web de confianza.** Muchas personas no saben cómo comprobar si un sitio web es seguro o no, por lo tanto, se darán algunos consejos:

1. En primer lugar, **comprueba si la URL tiene la ortografía correcta**, está asegurada con "https" y tiene algún tipo de indicador de que está verificada, como un signo de candado.
2. En segundo lugar, **los sitios web que parecen inseguros suelen serlo**. Si el propietario del sitio web no está invirtiendo en la apariencia y la experiencia del usuario, probablemente no esté invirtiendo en la seguridad del sitio. Por lo tanto, estos sitios son propensos al malware, que podría ser una amenaza para su seguridad.
3. En tercer lugar, **debes poder comprobar que hay información de contacto disponible, así como una política de privacidad accesible**. Suelen encontrarse en la parte inferior de la página de inicio. 4. Otro consejo útil es leer algunos testimonios y reseñas del sitio por parte de otras personas para que pueda conocer las experiencias que otras personas tuvieron al utilizar estos sitios web.

También hay otras prácticas que pueden poner en riesgo la seguridad digital como **el uso de WIFI públicas**. Es cierto que este servicio que prestan algunos hoteles y aeropuertos es gratuito, pero tiene un precio. Estos hotspots WIFI gratuitos permiten a los hackers situarse entre la persona que lo utiliza y el punto de conexión, por lo que en lugar de hablar directamente con el hotspot, la gente está enviando su información al hacker, que luego se basa en ella. Así, los piratas informáticos tienen acceso a toda la información que la gente envía por Internet: correos electrónicos importantes, datos de tarjetas de crédito y credenciales de seguridad. Una vez que los hackers tienen esa información, pueden acceder a tus sistemas como si fueran tú.

Para evitar que te hackeen de esta manera, es recomendable que mantengas el WIFI apagado cuando no lo necesites y cuando tengas que utilizar este tipo de conexiones lo hagas con una VPN. Una VPN es una red privada virtual ya que te ayudará a que tu información esté fuertemente encriptada. Si realmente necesitas usar este WIFI gratuito, intenta no hacer operaciones bancarias online, compras o trabajar. Algo que también puede ayudar es desactivar el Bluetooth y el intercambio de archivos.

¿Cómo pueden los individuos proteger sus datos personales?

1. **Asegure sus cuentas**

En la última década, las violaciones de datos y las filtraciones de contraseñas han golpeado a grandes empresas como Facebook, Home Depot, Marriott, Yahoo, etc., y las instituciones gubernamentales también han sufrido ciberataques a través de los cuales terceras partes no autorizadas han obtenido acceso a la información personal de los ciudadanos (por ejemplo, el ataque a la Agencia Nacional de Ingresos de Bulgaria en 2019).

Si tienes cuentas en Internet, es posible que los hackers hayan filtrado datos de al menos una de ellas. Para comprobarlo, puedes buscar tu dirección de correo electrónico en **Have I Been Pwned?** (https://haveibeenpwned.com/) para cotejarla con cientos de filtraciones de datos (*una "filtración" es un incidente en el que los datos quedan expuestos inadvertidamente en un sistema vulnerable, normalmente debido a controles de acceso insuficientes o a fallos de seguridad en el software*).

Hay otras formas de identificar posibles indicios de que una cuenta ha sido pirateada, su identidad robada o sus datos violados de alguna otra forma. Infórmese sobre las señales de advertencia de una posible violación y cree hábitos positivos para vigilar la seguridad de sus datos personales con el fin de identificar posibles ataques o violaciones antes de que se conviertan en una devastación. Lee consejos sobre protección de datos e información que describa las señales de advertencia habituales de una violación de datos o pirateo informático, como esta lista de "**15 señales de que te han pirateado y cómo defenderse**" (https://www.csoonline.com/article/3617849/15-signs-youve-been-hacked-and-how-to-fight-back.html)

Si su cuenta ha sido pirateada, sus datos perdidos o su dispositivo robado, considérelo una oportunidad de aprendizaje. Averigüe exactamente qué falló y cómo podría haber protegido sus datos tomando mejores precauciones. Mientras arregla las cosas, es un buen momento para dar un paso atrás y hacerse una pregunta más básica: ¿Cuál fue el motivo de la filtración? Si se trataba de su cuenta bancaria, la respuesta puede ser obvia.
En otros casos, como el del correo electrónico, puede deberse a un sinfín de motivos: desde utilizarlo para enviar spam hasta solicitar dinero a tus contactos o conseguir el restablecimiento de contraseñas en otros servicios. Un atacante puede incluso estar intentando acceder a su empresa. Saber por qué le han atacado también puede ayudarle a veces a entender cómo le han violado.

Una forma de aumentar el nivel de seguridad digital y proteger nuestros datos personales es **utilizar un gestor de contraseñas** para generar y recordar contraseñas diferentes y complejas para cada cuenta. Esta es una de las cosas más importantes que la gente puede hacer para proteger su privacidad y seguridad hoy en día. **LastPass** https://www.lastpass.com y **1password** (https://1password.com/) pueden ayudarte a hacerlo, generando contraseñas, supervisando las cuentas en busca de fallos de seguridad, sugiriendo el cambio de contraseñas débiles y sincronizando tus contraseñas entre el ordenador y el teléfono. **No utilices como contraseñas números de la Seguridad Social, números de teléfono, direcciones u otros datos de identificación personal.**

Otra sugerencia es utilizar también la autenticación en dos pasos siempre que sea posible para sus cuentas en línea. La mayoría de los bancos y las principales redes sociales ofrecen esta opción. Como su nombre indica, la autenticación en dos pasos requiere dos pasos: introducir tu contraseña e introducir un número al que sólo tú puedes acceder. Por ejemplo, el primer paso es iniciar sesión en Facebook con tu nombre de usuario y contraseña. En el segundo paso, Facebook te envía un código temporal en un mensaje de texto o, mejor aún, a través de una aplicación como Google Authenticator, y tú introduces ese código para iniciar sesión.

2. Proteja su navegación web

Las empresas y los sitios web rastrean todo lo que hacemos en Internet. Todos los anuncios, botones de redes sociales y sitios web recopilan información sobre su ubicación, hábitos de navegación y mucho más. Los datos recopilados revelan más sobre usted de lo que podría esperar. Incluso si no comparte su información personal públicamente en las redes sociales, es muy probable que los sitios web que visita con regularidad proporcionen todos los datos que los anunciantes necesitan para determinar el tipo de persona que es. Por eso, los anuncios dirigidos siguen siendo una de las innovaciones más inquietantes de Internet.

Una extensión del navegador como **uBlock Origin** (https://ublockorigin.com/) bloquea los anuncios y los datos que recopilan. La extensión uBlock Origin también evita que se ejecute malware en tu navegador y te ofrece una forma sencilla de desactivar el bloqueo de anuncios cuando quieras apoyar sitios que sabes que son seguros.

Puedes combinar uBlock con **Privacy Badger** (https://privacybadger.org/), que bloquea los rastreadores, y los anuncios no aparecerán en todas partes. Para ralentizar aún más los anuncios de acosadores, desactive los anuncios basados en intereses de Apple, Facebook, Google y Twitter. Muchos sitios web ofrecen medios para excluirse de la recopilación de datos, pero hay que hacerlo manualmente. Hacer esto no eliminará el problema por completo, pero reducirá significativamente la cantidad de datos recopilados.

Instalar la extensión **HTTPS Everywhere** (https://chrome.google.com/webstore/detail/https-everywhere/gcbommkclmclpchllfjekcdonpmejbdp) también ayuda a proteger su información personal. Te dirige automáticamente a la versión segura de un sitio cuando éste lo admite, lo que dificulta que un atacante, especialmente si estás en una Wi-Fi pública en una cafetería, aeropuerto u hotel, espíe digitalmente lo que estás haciendo.

3. **Utilice software antivirus en su ordenador**

Puede que los virus no parezcan tan comunes como hace una década, pero siguen existiendo. El software malicioso en su ordenador puede causar todo tipo de estragos, desde molestas ventanas emergentes hasta convertir la minería de bitcoin en un escáner de información personal. Si corre el riesgo de hacer clic en enlaces peligrosos, o si comparte una computadora con varias personas en un hogar, vale la pena configurar un software antivirus, especialmente en computadoras con Windows. Si su ordenador funciona con Windows 10, debería utilizar el software integrado de Microsoft, **Windows Defender**. También puedes tener una capa extra de protección si instalas un programa antivirus.

4. **Actualice su software y sus dispositivos**

Los sistemas operativos de teléfonos y ordenadores, los navegadores web, las aplicaciones más populares e incluso los dispositivos domésticos inteligentes reciben actualizaciones frecuentes con nuevas funciones y mejoras de seguridad. Estas actualizaciones de seguridad suelen ser mucho mejores para frustrar a los hackers que los antivirus.

Los tres principales sistemas operativos pueden actualizarse automáticamente, pero deberías tomarte un momento para comprobar que tienes las actualizaciones automáticas activadas para el sistema operativo que elijas: Windows, macOS o Chrome OS. Aunque es frustrante encender el ordenador y tener que esperar una actualización que podría romper el software que utilizas, las ventajas de seguridad merecen la pena. Tu teléfono también tiene opciones de actualización automática, pero a veces necesitas aprobar manualmente la instalación de actualizaciones.

5. **No instale software que no conozca y en el que no confíe plenamente**

Cada aplicación extraña que instalas en tu teléfono y cada extensión del navegador o programa que descargas de un sitio web sospechoso representa otro agujero potencial para tu privacidad y seguridad. Innumerables aplicaciones móviles rastrean tu ubicación allá donde vayas y recopilan tus datos sin pedirte consentimiento, incluso en aplicaciones para niños.

Es bueno saber qué aplicaciones tienen acceso a tu ubicación, contactos, micrófono y otros datos. Desactiva los permisos que no tengan sentido. Por ejemplo, Google Maps necesita tu ubicación para funcionar, pero tu aplicación de notas no. En el futuro, piensa en los permisos

de las aplicaciones cuando instales software nuevo; si una aplicación es gratuita, es posible que esté recopilando y vendiendo tus datos.

6. **Desactiva Bluetooth cuando no lo utilices**

La tecnología Bluetooth ha ofrecido increíbles comodidades al mundo móvil, pero también abre la puerta a las vulnerabilidades. La mayoría de las amenazas que se aprovechan de la conectividad Bluetooth dependen de la conexión Bluetooth activa y, aunque no suelen ser devastadoras ni peligrosas, son ciertamente incómodas y pueden ser graves. Los ataques Bluetooth dependen de la explotación del proceso de solicitud y concesión de permisos, que es la columna vertebral de la conectividad Bluetooth. Independientemente de las características de seguridad de su dispositivo, la única manera de evitar por completo que los atacantes exploten ese proceso de solicitud y concesión de permisos es apagar la función Bluetooth de su dispositivo cuando no lo esté utilizando; no ponerlo en un modo invisible o indetectable, sino apagarlo por completo.

7. **Ser demasiado cuidadoso a la hora de compartir información personal**

Este consejo se aplica tanto al mundo online como al offline: ¿quién te pide tus datos personales, como el número de la Seguridad Social o la información de tu tarjeta de crédito? ¿Para qué la necesitan? ¿Cómo la van a utilizar? ¿De qué medidas de seguridad disponen para garantizar la privacidad de tus datos? Todas estas importantes preguntas deben tener una respuesta clara antes de facilitar sus datos personales a nadie.

8. **Cuidado con los imitadores**

En relación con el consejo anterior, hay muchos impostores que intentan engañar a los consumidores desprevenidos para que faciliten su información personal sensible haciéndose pasar por el banco, la compañía de la tarjeta de crédito u otra entidad del individuo. **Esto puede ocurrir por teléfono o en línea, a través de correos electrónicos de phishing o sitios web diseñados para imitar el aspecto de la empresa auténtica.**

Asegúrese de saber quién recibe su información personal o financiera. No facilite información personal por teléfono, correo o Internet a menos que usted haya iniciado el contacto o sepa con quién está tratando. Si una empresa que dice tener una cuenta con usted le envía un correo electrónico pidiéndole información personal, no haga clic en los enlaces que contiene. En su lugar, escriba el nombre de la empresa en su navegador, vaya a

su sitio web y póngase en contacto con ellos a través del servicio de atención al cliente. O llame al número de atención al cliente que aparece en el extracto de su cuenta. Pregunte si la empresa ha enviado realmente una solicitud.

9. No compartas demasiada información en las plataformas de las redes sociales

Las redes sociales se han convertido en una forma de vida para muchas personas, pero compartir demasiada información personal en los perfiles de las redes sociales puede ser peligroso. Por ejemplo, muchos piratas informáticos han logrado adivinar contraseñas mediante métodos de ensayo y error, utilizando combinaciones de información común (como nombres de hijos, direcciones y otros detalles) que se encuentran fácilmente en los perfiles de redes sociales de los usuarios.

No publiques información que te haga vulnerable, como tu dirección o información sobre tus horarios o rutinas. Si tus contactos publican información sobre ti, asegúrate de que la información combinada no sea más de la que te sentirías cómodo si la conocieran extraños. Ten también cuidado al publicar información sobre tus contactos, incluidas fotos.

10. Personaliza la configuración de privacidad de tus redes sociales

Las redes sociales como Facebook permiten a los usuarios personalizar su configuración de privacidad. En Facebook, por ejemplo, puedes elegir quién puede ver el contenido que publicas y quién puede ver la información de tu perfil, como tu lugar de trabajo, fecha de nacimiento y ciudad de origen.

Elige siempre el mayor nivel de privacidad posible para asegurarte de que tus datos personales no acaban en manos de alguien malintencionado. El contenido que publiques en Internet permanecerá durante mucho tiempo, pero puedes personalizar la configuración de privacidad en la mayoría de las redes sociales. Esto afectará a quién puede ponerse en contacto contigo y quién puede ver la información que publicas.

Sé exigente: aunque es divertido compartir información, ten en cuenta tu reputación en Internet. Y si divulgas información públicamente en exceso, los ladrones de identidad podrían utilizarla para apropiarse de tu identidad.

11. No olvides cerrar la sesión

Iniciar sesión en los servicios en línea es necesario cuando necesitas acceder a tus cuentas personales, pero muchos usuarios olvidan cerrar la sesión cuando terminan de utilizar un servicio.

Cuando accedas a sitios web basados en cuentas a través de un ordenador público (o un dispositivo compartido), asegúrate de cerrar la sesión del servicio cuando ésta termine. El hecho de que se acceda a un nuevo sitio web tras una visita a un sitio en el que se ha iniciado sesión no significa que el siguiente usuario no pueda pulsar el botón de volver atrás y acceder a la cuenta en la que se ha iniciado sesión. Algunos sistemas también están configurados para guardar automáticamente la información, así que asegúrate de ver si esta función se puede desactivar.

12. No abras correos electrónicos de personas que no conoces

Si recibes un correo electrónico de una fuente o persona que no reconoces, no lo abras y, por supuesto, evita hacer clic en enlaces o archivos adjuntos.

Hay una regla de oro para tratar los mensajes de spam: si parece un mensaje de spam, probablemente lo sea; así que elimínelo sin hacer clic ni descargar nada. Estos mensajes pueden contener software que indica al remitente que usted ha abierto el correo electrónico, confirmando que tiene una cuenta activa, lo que puede dar lugar a más mensajes de spam. Algunos programas maliciosos pueden robar tu dirección de correo electrónico y utilizarla para reenviar mensajes de spam bajo la apariencia de una dirección legítima. Por ejemplo, los impostores podrían hacerse pasar por alguien que usted conoce, como un amigo, un pariente o un colega. Si el mensaje en cuestión parece proceder de alguien que conoces, ponte en contacto con él fuera de tu correo electrónico.

13. No guardes contraseñas en tu navegador

La práctica habitual de "recordar contraseñas" en los navegadores es peligrosa. De hecho, si alguien consiguiera acceder a tu ordenador o dispositivo móvil, podría acceder fácilmente a cualquier cuenta para la que hayas almacenado credenciales de inicio de sesión en tu navegador. Aunque puede hacer que el inicio de sesión sea más cómodo, es un hábito arriesgado en términos de protección de datos. Estate atento a estas ventanas emergentes y asegúrate de rechazarlas.

14. No utilices credenciales de redes sociales para registrarte o iniciar sesión en sitios de terceros.

Parece una opción muy práctica: Sólo tienes que registrarte en un sitio web o servicio en línea utilizando tu cuenta de Facebook o LinkedIn y, siempre que hayas iniciado sesión en esa red social, acceder al sitio de terceros es rápido y sencillo. Sin embargo, hacerlo puede poner en peligro tu privacidad.

Aunque es una opción cómoda, iniciar sesión en otra cuenta con tu nombre de usuario y contraseña de Facebook puede significar dar al otro sitio toda la información que Facebook ha recopilado sobre ti. Peor aún, si alguien secuestra tu información de inicio de sesión social, también puede obtener acceso a estas cuentas de terceros.

15. Elige un proveedor de correo electrónico seguro y de confianza

Asegúrese de que tu proveedor de correo electrónico garantiza la seguridad adecuada. Debes asegurarte de que tu proveedor de correo electrónico utiliza tecnología como **DMARC** para detener el phishing y minimizar los riesgos. La buena noticia es que Google lo hace, Yahoo lo hace, Microsoft lo soporta, AOL lo soporta, así que si estás en uno de ellos, estás en camino de minimizar los riesgos de privacidad y seguridad.

4. Educación no formal

4. EDUCACIÓN NO FORMAL

En esta sección mencionaremos contextos nacionales de formas no formales de concienciación sobre el ciberacoso y el discurso del odio.

- **Países Bajos**

Hay otras formas no formales de concienciar a la gente sobre cuestiones relacionadas con la seguridad en Internet. No solo se habla de ciberseguridad en la educación formal o específica; a través de **noticias, personas influyentes en línea, padres y profesores**, y víctimas que hablan, la concienciación aumenta de diferentes maneras.

Ciberseguridad y privacidad

Abordar o regular la ciberseguridad y la privacidad suele asociarse a instituciones y organismos oficiales o a la educación formal. Sin embargo, la educación no formal al respecto también influye.

Chantal Stekelenburg (https://twitter.com/mifare_lady) is part of the **Women in Cybersecurity Community Association (WICCA)** (https://womenofwicca.nl/) and has gained a large online following. She has spoken out about cybersecurity and mainly focuses on encouraging women to become security enthusiasts and experts.

Chantal Stekelenburg (https://twitter.com/mifare_lady) forma parte de la asociación **Women in Cybersecurity Community Association (WICCA)** (https://womenofwicca.nl/) y ha conseguido un gran número de seguidores en Internet. Ha hablado sobre ciberseguridad y se centra principalmente en animar a las mujeres a convertirse en entusiastas y expertas en seguridad.

Cyberbullying

Las personas influyentes y otros individuos que han hablado sobre el ciberacoso han tenido un efecto importante en la forma en que la gente ve este problema y en cómo se educa al respecto. Muchos jóvenes se avergüenzan a menudo de hablar de manera formal u oficial, presentando informes o alertando al personal de la escuela o de otras instituciones. Por ello,

los enfoques no formales son útiles, ya que permiten a las personas que han sufrido ciberacoso relacionarse con otras, sentirse menos solas y más dispuestas a denunciar.

Una noticia de 2018 informaba de que un tribunal de apelación holandés confirmaba la pena de prisión para un hombre condenado por ciberacoso a muchos jóvenes, hombres y mujeres, muchos de ellos de los Países Bajos. Había presionado a chicas para que realizaran actos sexuales delante de cámaras web. Esta historia acaparó mucha atención en los medios de comunicación y puede considerarse un claro ejemplo de educación no formal en materia de ciberacoso y ciberdelincuencia. Esencialmente, **cuanta más atención se preste a casos como éste, mayor será la concienciación y mejor preparada estará la gente para prevenirlos y denunciarlos.**

Discurso de odio

La importancia de la educación no formal se extiende a la incitación al odio, ya que es vital que la gente se manifieste en contra. Ha habido importantes campañas basadas en este tema.

Existe una campaña nacional en los Países Bajos, que forma parte de **la Campaña Juvenil No Hate Speech** (https://www.coe.int/en/web/no-hate-campaign) del Consejo de Europa, cuyo objetivo es movilizar a los jóvenes para combatir la incitación al odio y promover los derechos humanos. Esto anima a la gente a denunciar la incitación al odio y a combatirla directamente. De este modo, los activistas en línea disponen de una plataforma y una comunidad donde compartir ideas y unirse contra este problema, capacitando a la gente para denunciar la incitación al odio.

- **España**

Cuando se habla de formas de educación no formal para concienciar sobre el ciberacoso y el discurso del odio en España, es imposible no mencionar el importante papel de la cultura, los influencers y las grandes campañas de marketing.

Ciberacoso

Los influencers son sin duda una referencia potencial para la gente. Con millones de seguidores, esta nueva profesión es capaz de llegar a un público más amplio a través de las redes sociales y las plataformas en línea. La metodología es sencilla y eficaz, mientras las personas consumen medios sociales durante su tiempo libre, también reciben toda esta información transmitida por los influencers sin hacer ningún esfuerzo adicional.

En España hay muchos ejemplos de influencers que han utilizado su protagonismo para concienciar sobre el ciberacoso. Por ejemplo, **Y luego ganas tú (Nube de Tinta)** es un libro de relatos cortos en el que los autores (5 influencers españoles) cuentan, a través de sus propias historias y ficciones que beben de la realidad, el problema del acoso escolar.

Un problema que se nos está yendo de las manos como sociedad: uno de cada dos estudiantes en España afirma haber sufrido algún tipo de bullying o ciberbullying. Estos influencers son Javier Ruescas (@javier_ruescas), Manu Carbajo (@karbajo), Jedet Sánchez (@lajedet), María Herrejón (@hersimmar) y Andrea Compton (@andreacomptonn). Son populares en España por su lucha por los derechos sociales y la visibilidad.

Otro ejemplo de lucha contra el ciberacoso es el podcast **Estirando el chicle** (https://www.youtube.com/c/Estirandoelchicle?app=desktop) conducido por Carolina Iglesias y Victoria Martín. En este podcast se entrevista a múltiples personajes famosos sacando a relucir temas como el ciberacoso o la visibilidad LGBTIQA+. De hecho, el podcast ha obtenido un gran reconocimiento con premios como el Premio Ondas al mejor podcast o programa de difusión digital por ser "*un programa rompedor en cuanto a lenguaje y enfoque que mezcla humor, entrevistas y contenido social sin prejuicios*".

In addition, it would also be relevant to mention how the famous shampoo brand H&S has also contributed to the fight against bullying. In the campaign **'Stop bullying'** (https://www.hys.es/es-es/frena-el-bullying/) many spanish public figures, like Marta Pompo or Ibai, attempt to raise awareness by telling their own experiences with hate speech in

social media. In addition, an educational microsite will be activated on the H&S website with advice for pupils, teachers and parents to get them to take an active role in bullying situations. As well as information pills to raise awareness among the different parties involved.

Además, también sería relevante mencionar cómo la famosa marca de champú H&S también ha contribuido a la lucha contra el bullying. En la campaña "**Stop bullying**" (https://www.hys.es/es-es/frena-el-bullying/) muchos personajes públicos españoles, como **Marta Pompo o Ibai**, intentan concienciar contando sus propias experiencias con el discurso del odio en las redes sociales. Además, se activará un microsite educativo en la web de H&S con consejos para alumnos, profesores y padres para que adopten un papel activo ante situaciones de acoso. Así como píldoras informativas para sensibilizar a las distintas partes implicadas.

- **Bélgica**

Desde Bélgica, queremos destacar una campaña de comunicación contra el ciberacoso de los jóvenes y destacar a uno de sus principales influenciadores:

Campaña 'WAT TEGEN WAT PESTEN'

La plataforma juvenil **WAT WAT** (https://www.watwat.be/) colabora con personas influyentes y jóvenes para debatir sobre el acoso entre los jóvenes a través de consejos y experiencias. Con un juego de dilemas en Facebook messenger, WAT WAT desata la conversación sobre el acoso ("*Acosar o ser acosado, trolear o gustar, matón o cabeza de chorlito: la elección es tuya*").

Desarrollaron una campaña durante la "Semana contra el acoso" flamenca para concienciar a niños y jóvenes sobre qué es el acoso, qué se puede hacer al respecto y qué consecuencias tiene. Se compartieron públicamente historias reales: Angel (16) fue obligada por sus acosadores a comer residuos de GFT. En la semana contra el acoso ella, junto con Yasmien Naciri (27), Margot (22) y Jorrit (23), compartió su historia y mostró sus cicatrices de años de acoso. Estas valientes historias animan a los jóvenes a reflexionar, a hablar del tema y a ayudarse mutuamente.

WAT WAT hace un llamamiento a todos para que hagan más contra el acoso, como por ejemplo, hacer una declaración colgando los carteles de la campaña en las aulas o salas juveniles y hacer del acoso un tema de debate en grupo con la metodología de juego con el hashtag #tegenpesten (#otravezcontraelacoso).

Por otro lado, **Angèle** (angele_vl), la cantante belga con más éxito del momento, es también la influencer más seguida en Instagram del país con 3,6 millones (Statista, 2019). No solo eso, la artista está bastante comprometida con la educación igualitaria y el fin de los discursos de odio contra las mujeres y la comunidad LGTBI+, y eso se refleja en sus canciones.

- **Bulgaria**

El ciberacoso se ha abordado a través de varias campañas y organizaciones en línea que trabajan para su prevención y para concienciar a jóvenes, padres y profesores sobre este problema social. Un ejemplo de este tipo de campaña en línea son las Directrices sobre el ciberacoso elaboradas por **Safenet.bg** (https://cyberbullying.safenet.bg/).

Aquí, de forma muy visual, los jóvenes pueden ver ejemplos de ciberacoso y compartir si han experimentado algo similar; pueden denunciar un incidente a través del enlace proporcionado. También pueden leer información útil, consejos y sugerencias sobre el ciberacoso y cómo reaccionar ante él.

Safenet.bg también tiene un canal en YouTube (https://www.youtube.com/@safenetbg948) donde hay vídeos relacionados con el ciberacoso, la incitación al odio en la red, etc., con el objetivo de concienciar a los jóvenes sobre estos temas de una forma más atractiva y visual.

La empresa de telecomunicaciones **Yettel** también tiene un canal de YouTube (https://www.youtube.com/@YettelBulgaria) desarrollado en 2020, donde hay diversos vídeos para jóvenes con información sobre diferentes riesgos en línea a los que pueden enfrentarse los jóvenes, como perfiles falsos, ciberacoso, enlaces peligrosos, riesgos en TikTok y YouTube, en juegos, etc.

5. Conclusiones

5. CONCLUSIONES

A lo largo de este manual se han explicado y contextualizado el ciberacoso, el discurso del odio, la ciberseguridad y la privacidad. Sus definiciones pueden variar a lo largo de los diferentes países, sin embargo, se consideran como una agresión a otras personas. En el caso del Ciberacoso normalmente hay tres protagonistas (el agresor, la víctima y los espectadores), en el caso del Discurso de Odio, es más difícil establecer un escenario común, pero implica por igual a una persona que discrimina y al receptor que es discriminado.

Este manual incluye diferentes formas de identificar, tratar y denunciar el ciberacoso y la incitación al odio, por supuesto, dependerá de quién sea la víctima (tú mismo, un compañero, tus hijos, etc.) pero también del marco legal del país. Por ejemplo, en España se puede denunciar a la policía, mientras que en los Países Bajos existe una línea nacional de ayuda contra la discriminación. Además, se muestra por qué conceptos como la protección de datos o la tríada CIAD son importantes, así como los tipos de amenazas a la privacidad, como el robo de identidad, el acoso sexual en línea, el phising o los fraudes.

En conclusión, este documento no sólo ofrece definiciones o conceptos clave sobre el ciberacoso, la incitación al odio, la ciberseguridad y la privacidad, sino que también sirve de guía para prevenir, reaccionar y denunciar este tipo de abusos.

6. Referencias

6. REFERENCIAS

101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Online Safe in 2022. (2022, May 26). Digital Guardian. https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe

A, D. (2020). *Cyberbullying (for Parents) - Nemours KidsHealth*. Nemours KidsHealth. https://kidshealth.org/en/parents/cyberbullying.html

A. (2018). *Report security vulnerabilities | TikTok Help Center*. TikTok. https://support.tiktok.com/en/safety-hc/reporting-security-vulnerabilities/reporting-the-security-vulnerabilities.

Assistant Secretary for Public Affairs (ASPA). (2019b, December 4). *Report Cyberbullying*. StopBullying.Gov. https://www.stopbullying.gov/cyberbullying/how-to-report

Assistant Secretary for Public Affairs (ASPA). (2021, May 21). *Tips for Teachers*. StopBullying.Gov. https://www.stopbullying.gov/cyberbullying/tips-for-teachers

C, S. (2021). *Password security: How to create strong passwords in 5 steps*. Norton. https://us.norton.com/internetsecurity-privacy-password-security.html.

Caroline Rizza. (2013). *Social networks and Cyber-bullying among teenagers: EU Scientific e political report*. https://doi.org/10.2788/41784

Celine Chateau. (2016). *Policy department Citizen¡s rights and constitutional affairs*. https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf

Center, C. R. (2021, October 18). *Preventing Cyberbullying: Top Ten Tips for Adults Who Are Being Harassed Online*. Cyberbullying Research Center. https://cyberbullying.org/preventing-cyberbullying-adults

CISCO. (2021). *Think Before You Click [Slides]*. CISCO. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/phishing-program-infographic.pdf

Commission for Personal Data Protection, available. (2019). FOLD. https://www.cpdp.bg/?p=element&aid=12

Convention on Cybercrime (No. 185). (2001, November). Convention on Cybercrime. https://rm.coe.int/1680081561

Cyberbullying Research Center. (2022). *Cyberbullying Fact Sheet: Identification, Prevention, and Response*. https://cyberbullying.org/cyberbullying-fact-sheet-identification-prevention-and-response

Defining online sexual harassment. (2021, December 15). Childnet. https://www.childnet.com/what-we-do/our-projects/project-deshame/defining-online-sexual-harassment/

Digital Guardian. (22–05-26). *101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Online Safe in 2022*. https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe.

Facebook - Meld je aan of registreer je. (2018). Facebook. https://www.facebook.com/unsupportedbrowser

Griffin, M. (2020, March 5). *Advice on what to do if your child is a victim of cyberbullying*. Laya Healthcare. https://www.layahealthcare.ie/thrive/family/what-to-do-if-your-child-is-victim-of-cyber-bullyi/.

How to Protect Your Digital Privacy. (2019). The Privacy Project Guides - The New York Times. https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy

Identity Theft. (2022, June 12). Investopedia. https://www.investopedia.com/terms/i/identitytheft.asp

Instagram Help Center. (2018). Instagram. https://help.instagram.com/192435014247952?helpref=uf_permalink

J. (2013). *Social Networks and Cyber-bullying among Teenagers*. JRC Publications Repository. https://publications.jrc.ec.europa.eu/repository/handle/JRC80157

L. (2021, 28 enero). *Ciberdelincuencia en el código penal - Letslaw*. LetsLaw. https://letslaw.es/ciberdelincuencia/

L.J. (2022, June 2). *Delitos en redes: de cinco años de cárcel a multas de hasta 2.700 euros*. Diario Noticias de Álava. https://www.noticiasdealava.eus/vivir-on/internet-y-ciencia/2022/04/24/delitos-redes-consecuencias/1183252.html.

Lex.bg - P—P°PєPsPSPë, PïCЂP°PIPëP»PSPëC†Pë, PєPsPSCЃC,PëC,CґC†PëCЏ, PєPsPґPµPєCЃPë, PґCЉCЂP¶P°PIPµPS PIPµCЃC,PSPëPє, PïCЂP°PIPëP»PSPëC†Pë PïPs PïCЂPëP»P°PiP°PSPµ. (2017). Lex.Bg. https://www.lex.bg/laws/ldoc/1589654529

P. (2020). *Why is Data Protection Important?* PECB. https://pecb.com/article/why-is-data-protection-important

S, G. Cyberstalking: Prevention, Consequences, and Coping. (2021, August 17). Verywell Mind. https://www.verywellmind.com/what-is-cyberstalking-5181466

Safety and security. (2018). Twitter. https://help.twitter.com/en/safety-and-security

W, The Dangers of Hacking and What a Hacker. (2020). © Copyright 2004 - 2022 Webroot Inc. All Rights Reserved. https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats-hackers

What Is Internet Fraud? Types of Internet Fraud. (2019). Fortinet. https://www.fortinet.com/resources/cyberglossary/internet-fraud

What is personal data? (2018, August 1). European Commission - European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

What Is Phishing? (2022, May 5). Cisco. https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#%7Ehow-phishing-works

Wilkey Oh, E. (2020, March 15). *Teachers' Essential Guide to Cyberbullying Prevention*. Common Sense Education. https://www.commonsense.org/education/articles/teachers-essential-guide-to-cyberbullying-prevention

Ф. (2009). *Киберсигурност*. Фондация. https://www.netlaw.bg/bg/a/kiber-sigurnost

Si quieres saber más sobre #Digitsafe, visita nuestra web www.digit-safe.com

O póngase en contacto con nosotros en info@digit-safe.com

www.digit-safe.com
info@digit-safe.com