Seguridad, privacidad e identidad digital

Pedro Joel Maldonado Colón
Auxiliar de Sistemas de Información
17 de noviembre de 2020

Seguridad Informática

- **¿Qué es un sistema informático?**
  - Es el conjunto que resulta de la integración de cuatro elementos: hardware, software, datos y usuarios.
- **¿Cuál es el objetivo de integrar estos elementos?**
  - Hacer posible el procesamiento automático de los datos.
- **¿Qué son datos?**
  - Los datos son la materia prima que procesamos para producir información.
- **¿Qué es la información?**
  - El resultado de procesar o transformar los datos.

Principios de Seguridad Informática

- **La Seguridad Informática:** se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos.

- **Para lograr sus objetivos, la seguridad informática se fundamenta en tres principios:**
  - Confidencialidad
  - Integridad
  - Disponibilidad

Amenazas

- **Las amenazas pueden ser causadas por:**
  - Usuarios
  - Programas maliciosos
  - Errores de programación
  - Intrusos
  - Un siniestro
  - Personal técnico interno
  - Fallos electrónicos o lógicos
  - Catástrofes naturales

Amenazas más comunes

- Spam
- Farming
- Phishing
- Ransomware
- Gusano informático
- Spyware / Trojan Horse
- Ataque distribuido de denegación de servicio
- Red de equipos zombie
- Malware
- Virus
- Ciberacoso

Privacidad digital

- Este término se refiere al derecho de los usuarios a proteger sus datos en la red y decidir qué información está visible para el resto.

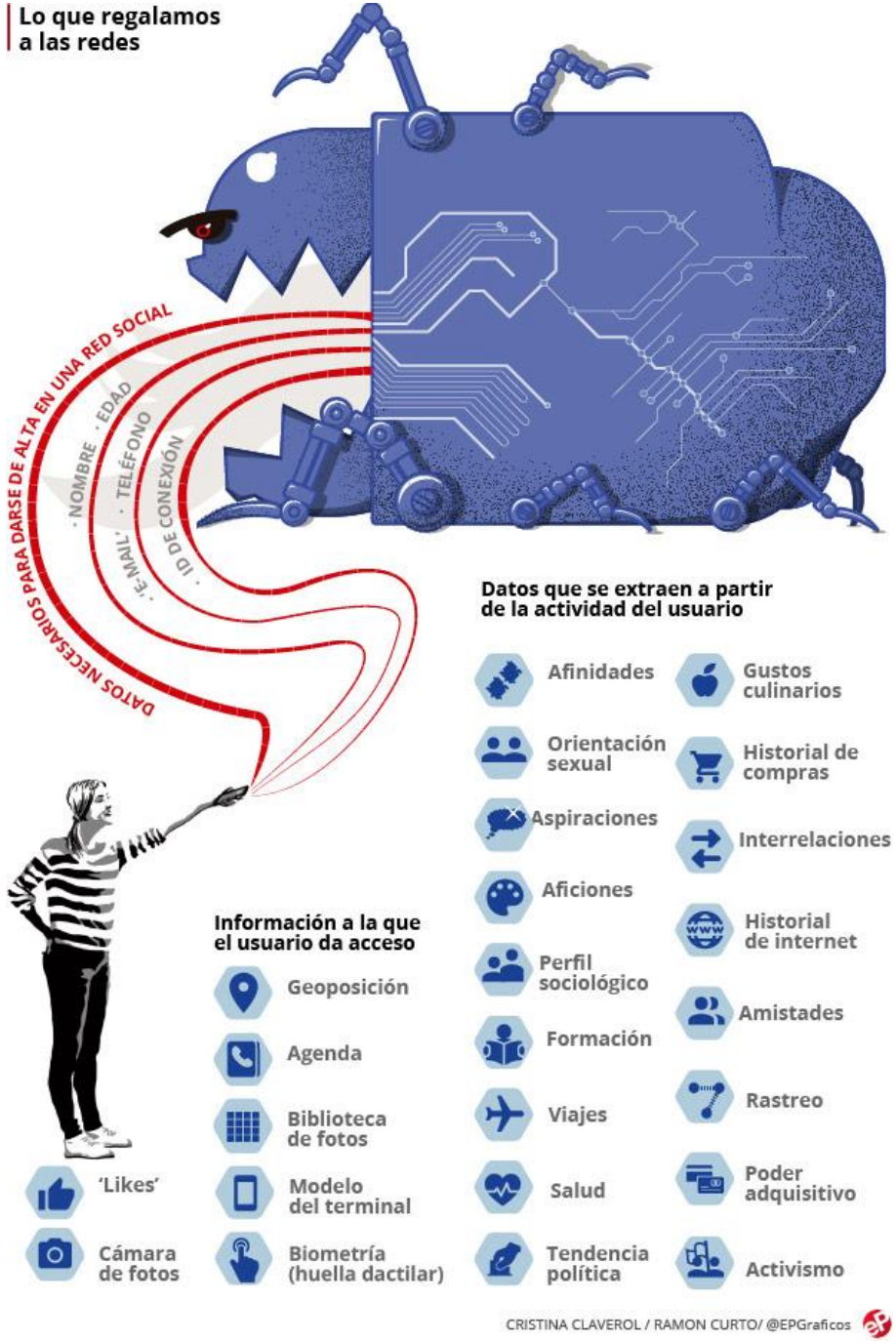
- El **concepto de privacidad digital** es relativamente joven, ya que está unido a la aparición y desarrollo de internet y las telecomunicaciones. De hecho, hasta hace poco no existía una regulación clara al respecto.

¿Qué redes sociales son las más utilizadas?

- De todas ellas, el TOP 5 de redes sociales con mayor número de usuarios en el mundo son:
- **Facebook**: 2.271 millones de usuarios
- **YouTube**: 1.900 millones de usuarios
- **WhatsApp**: 1.500 millones de usuarios
- **Facebook Messenger**: 1.300 millones de usuarios
- **WeChat**: 1.083 millones de usuarios
- El país en el que mayor inserción de las redes sociales hay entre su población es Emiratos Árabes Unidos, ¡99% de inserción! Es decir, el país con el mayor volumen de usuarios activos en las redes respecto al total de la población.

Privacidad en redes sociales

- **Ingeniería social**
  - Test
  - Juegos
  - Concursos
  - Encuestas
- **Big data**
- **Machine Learning**
- **Web scraping**
- **Cookies**



¿Para qué se usan los datos?

- Recoger datos para márketing
- Crear perfiles avanzados con información más compleja
- Captar datos para luego hacer 'phishing' y demás
- Segmentación e hipersegmentación de audiencias para publicidad
- Retargeting
- Personalizar los anuncios como las publicaciones que nos muestra
- Data brokers

Motores de búsqueda

- **Lo que recogen:**
  - Todos los datos que conciernen las búsquedas, la geolocalización u otros datos consultados.
- **Lo que venden:**
  - Al igual que las redes sociales, sus ingresos provienen en gran parte de la publicidad. No venden datos, sino el acceso a un consumidor de características muy precisas, fruto del cruce de datos del motor de búsqueda, pero también en el caso de Google, de todas las búsquedas y contenidos vistos en YouTube, su filial.
- **Lo que comparten:**
  - Abren las puertas a otros programadores, a las aplicaciones y a las redes sociales.

Ventajas de la privacidad digital

- Aumentar la seguridad de la información y proteger frente a fraudes, ciberataques como “hackeos” o suplantación de identidad.
- Permitir que solo accedan a nuestros datos aquellos usuarios, empresas o proveedores de servicios a los que hayamos otorgado nuestro consentimiento.
- Adecuar a nuestro perfil y nuestros intereses los contenidos, productos o servicios que se nos ofrecen.
- Concienciar cada vez más a la gente sobre la importancia de proteger los datos personales en internet.

Desventajas de la privacidad digital

- Internet es una red inmensa, tratar de controlar todo el flujo de información no es un objetivo realista.
- Entra en conflicto con los intereses de grandes empresas y corporaciones.
- Todavía existe mucha gente que no comprende la importancia de proteger la información digital. Muchas personas siguen aceptando términos y condiciones de uso sin leerlas.
- A las generaciones pasadas les cuesta adaptarse a las nuevas exigencias en este campo, ya que la era digital avanza rápidamente y no espera por nadie.

Consejos de seguridad general

- Mantener el sistema operativo actualizado
- Gestores de contraseñas/No compartas tu información
- La importancia del segundo factor de autenticación
- Usar VPN
- Protocolo de seguridad HTTPS (páginas con candados)
- Utilizar páginas confiables/leer términos y condiciones
- Desinstalar aplicaciones
- Servicios de geolocalización
- Email (verificar enlaces de remitente)
- User profiles
- Controles (evitar redes públicas)
- Tener sentido común

Consejos de seguridad en redes sociales

- Divulgación de información personal
- Mantener información privada
- Las imágenes (y sus leyendas) hablan más de mil palabras
- Privacidad seleccionable
- Cuidado con el GPS y la localización
- Una clave fuerte, la primera defensa (doble factor)
- No guardar contraseñas
- Sistema de seguridad
- Protege tu identidad digital. Vigila la suplantación.

Ejemplos

- **Este es el tiempo que tardarían en romper algunas contraseñas del tipo:**
- abc1234: 1 milisegundo
- Toby2019: 4 segundos
- 28121999Mc: 2 horas
- Champions-League: 3 días
- WKTSLE1&: 47 años
- Meencantatomarcafe4vecesaldia: 102.133.402.054.325.310 siglos

Identidad digital

- **Identidad digital**
  - Es el rastro que cada usuario de *Internet* deja en la red como resultado de su interrelación con otros usuarios o con la generación de contenidos.

- **Comunicación 2.0**
  - Si matizamos en la comunicación 2.0 es aquella que gestionan las organizaciones y marcas en el entorno digital para optimizar y generar su reputación corporativa.
  - Por tanto, toda comunicación digital que se establezca por redes sociales, sitio web, blogs o plataformas e-commerce, e-mailing, foros…

- **Web 2.0**
  - Es un concepto que empezó a utilizarse en el año 2003. Su aparición se debió al auge de diversas aplicaciones como los blogs o las redes sociales, que permitieron que los usuarios dejaran de ser mejor sujetos pasivos para adoptar un rol mucho más activo y dinámico.

Elementos que conforman la identidad digital

- Perfiles personales
- Comentarios
- Contenidos digitales
- Contactos
- Las direcciones de correo electrónico
- La mensajería instantánea

Personal branding

- Nos referimos a la estrategia de atribuir a los profesionales una serie de cualidades que les diferencia de otros y sean posibles mantener en el tiempo.

- Es todo aquello que nos hace **únicos, diferentes, relevantes y especiales**; y que damos a conocer a nuestro público objetivo.

Reputación Online

- Por el término reputación, entendemos "*la opinión que otros tienen de una empresa, marca o persona*". Ésta puede ser positiva o negativa, en función de la experiencia que los demás hayan tenido o de los valores que la misma trasmite a la sociedad.

- Con la aparición del ecosistema 2.0, la reputación de un individuo o empresa también se ve reflejada en la red.
  - Reputación online negativa
  - Reputación online positiva

¿Cómo borrar contenido de internet?

- Unión Europea
- Derecho al olvido de Google
  - Según sentencia del Tribunal de Justicia de la UE de 13 de mayo de 2014, Google está obligado a borrar de sus búsquedas los resultados que contengan datos personales de un usuario, pero no implica que desaparezca de la página donde esté publicado. Para ello, deberemos ponernos en contacto, siempre y cuando sea posible, con el editor del sitio web.
- Estados Unidos
- En general, el 'derecho al olvido' se toma en EE.UU. como una limitación a la libertad de expresión.
  - Ley de Telecomunicaciones, que daría a empresas como Google, inmunidad sobre la responsabilidad del contenido en su servicio. "Según la legislación actual en EE.UU., Google no sería responsable"

¿Cómo borrar contenido de internet?

- Todos los buscadores incluyen un formulario de solicitud del contenido que queremos que sea eliminado de los resultados de búsqueda.

- La edad mínima para que los menores puedan prestar consentimiento para tratar sus datos personales en internet es de 14 años. Antes de esa edad, el consentimiento debe ser otorgado por sus padres o tutores.

- Los familiares o herederos de una persona, pueden solicitar que se elimine la información personal del fallecido, siempre y cuando éste no lo haya prohibido expresamente en vida.

Límites y Regulaciones

- En Estados Unidos no existe casi ninguna ley que proteja la utilización de datos provenientes de las redes sociales o motores de búsqueda.
  - La autoridad reguladora, la Federal Trade Commission (FTC), las vigila y ha sancionado a Facebook a partir de 2011 por su gestión de datos personales. También concluyó un acuerdo con Google en 2013, por prácticas que atentaban contra la competencia.

Ley de protección de datos (UE)

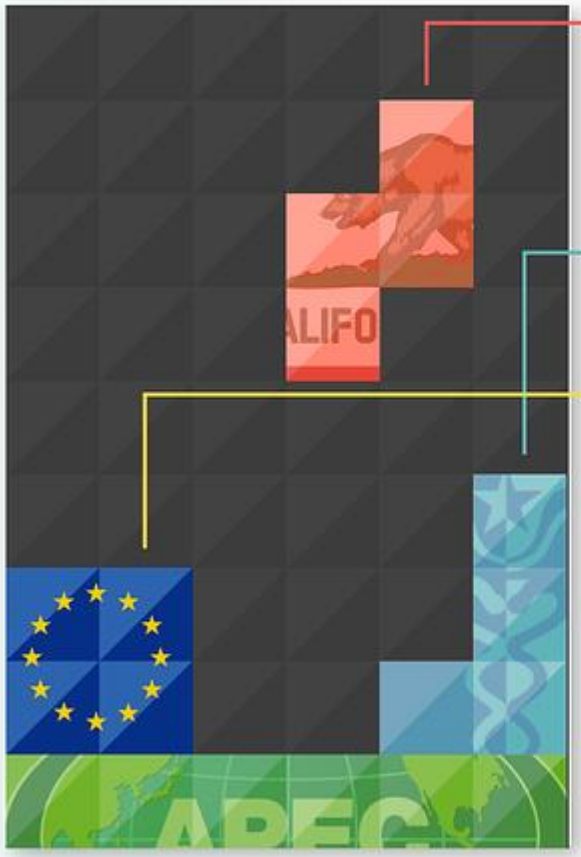
- El Reglamento General de Protección de Datos (GDPR) se promulgó en abril de 2016 y entró en vigencia el 25 de mayo de 2018.

- El GDPR se aplica a cualquier forma de datos personales.

- El GDPR se aplica a cualquier organización que recopile, almacene o procese los datos personales de los residentes de la UE, ya sea que la organización se base o no en la UE.

US Privacy Laws

NOT YET A UNIFIED SYSTEM



California's **CPA**, echoing the EU's GDPR, goes into effect in 2020

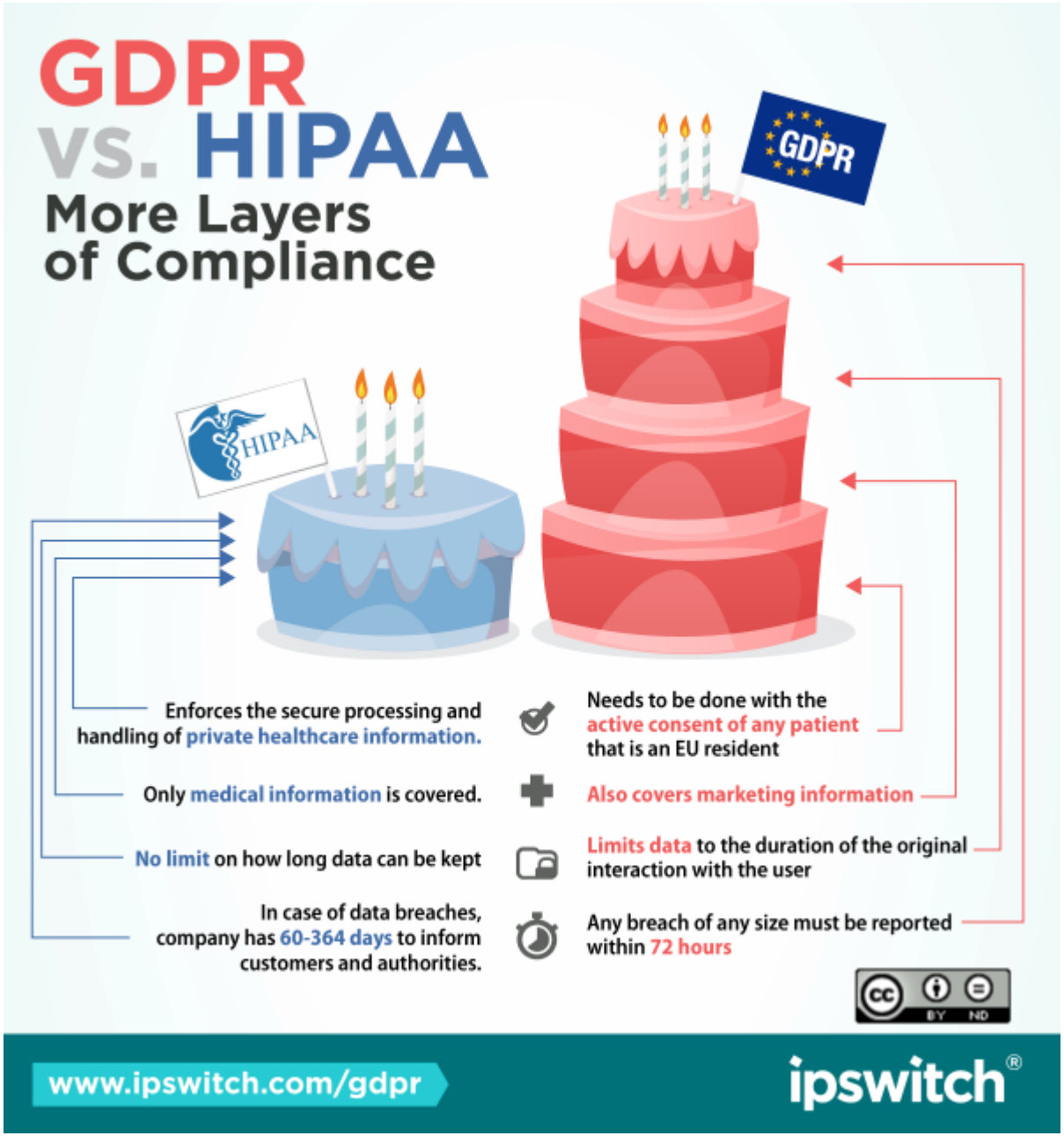
US **HIPAA** laws protect patient data

EU's **GDPR** applies to EU personal data, even when collected by US companies

The US agreed to **APEC's Cross-Border Privacy Rules (CBPR)** in July 2012, providing basic protections

www.ipswitch.com/privacy

Progress | ipswitch


GDPR
vs. HIPAA
More Layers of Compliance
GDPR
HIPAA
Enforces the secure processing and handling of private healthcare information.
Only medical information is covered.
No limit on how long data can be kept
In case of data breaches, company has 60-364 days to inform customers and authorities.
Needs to be done with the active consent of any patient that is an EU resident
Also covers marketing information
Limits data to the duration of the original interaction with the user
Any breach of any size must be reported within 72 hours
www.ipswitch.com/gdpr
ipswitch®

Identificación biométrica

- En los Estados Unidos, no existe una ley federal única e integral que regule la recopilación y el uso de datos biométricos. Sin embargo, Washington, después de Illinois y Texas, aprobó una ley de privacidad biométrica en junio de 2017.

- Las agencias gubernamentales y los grupos industriales han desarrollado pautas de autorregulación, extraídas de las mejores prácticas y que ahora son tenidas en cuenta por los reguladores.

Identificación biométrica

- A partir de julio de 2017, es legal en 47 estados que el software identifique a un individuo a través de imágenes tomadas sin consentimiento mientras está en público. Illinois y Texas no lo permiten para uso comercial.

- Esta ley cubre cualquier entidad comercial que recolecta identificadores biométricos con fines comerciales.

- El reconocimiento facial, por ejemplo, se puede realizar discretamente a distancia sin que el individuo proporcione información activamente.

Puerto Rico

- El 7 de septiembre de 2005 se aprobó la “Ley de Información al Ciudadano sobre la Seguridad de Bancos de Información” (“Ley Núm. 11-2005”) con el propósito de proteger a los ciudadanos residentes en Puerto Rico, víctimas de la usurpación de su identidad.

- Ley de Notificación de Política de Privacidad y el Reglamento para Implantar la Publicación de la Política de Privacidad en el Manejo de Datos Privados y Personales de Ciudadanos, según Recopilados por Comercios en Puerto Rico

Día Internacional de la Seguridad de la Información

- **Se celebra:** 30 de noviembre de 2020
- **Proclama:** Association for Computing Machinery (ACM)
- **Desde cuándo se celebra:** 1988

¡Gracias!

@bibliotecasagradooficial

Refererencias

Ático 34. (8 de mayo de 2020). *Identidad digital 2020, derechos asociados y cómo protegerla.* https://protecciondatos-lopd.com/empresas/identidad-digital/

Campillo-Alhama, C., & Martínez-Sala, A. M. (2017). Comunicación integrada 2.0 en la administración municipal. *El profesional de la información, 26*(3), 507-515. https://recyt.fecyt.es/index.php/EPI/article/view/58738

Carbellido, C. (6 de febrero de 2020). *Identidad digital, reputación online, el derecho al olvido y cómo borrar contenido de internet.* Un Community Manager. https://www.uncommunitymanager.es/identidad-digital/

Emi E. (2020). *¿Que es la ciberseguridad? 5 consejos para el 2020.* Medium. https://medium.com/@emiedre/que-es-la-ciberseguridad-5-consejos-para-2020-6083b0a588cb

González Ramírez, T., & López Gracia, A. (2018). La identidad digital de los adolescentes: usos y riesgos de las Tecnologías de la Información y la Comunicación. *Revista Latinoamericana Tecnología Educativa, 17*(2), 73-85. https://relatec.unex.es/article/view/3319

Hurtado, M. M., & Céspedes, L. (2017). Identidad en[red]ada: adolescentes que se construyen en la era digital. *De Familias y Terapias,* 43, 105-127.

Jané, C. (16 de abril de 2018). Qué saben las redes sociales de ti y para qué lo usan. *El Periódico.* https://www.elperiodico.com/es/sociedad/20180413/datos-redes-sociales-utilizacion-metodos-6755900

Jiménez, J. (23 de diciembre de 2017). *10 consejos para garantizar la seguridad en redes sociales.* Redes Zone. https://www.redeszone.net/2017/12/23/10-consejos-garantizar-la-seguridad-redes-sociales/

Refererencias

Moreno Bobadilla, A. (2019). El derecho al olvido digital: una brecha entre Europa y Estados Unidos. *Revista de Comunicación, 18*(1), 259-276. https://dialnet.unirioja.es/servlet/articulo?codigo=6838315

OBS Business School. (s.f.). *10 amenazas informáticas en el punto de mira.* https://obsbusiness.school/es/blog-investigacion/propiedad-intelectual-y-seguridad-de-la-informacion/10-amenazas-informaticas-en-el-punto-de-mira

Palou, N. (30 de abril de 2019). *Los temas de ciberseguridad que más preocupan a los expertos.* Economía Digital. https://www.economiadigital.es/tecnologia-y-tendencias/los-temas-de-ciberseguridad-que-mas-preocupan-a-los-expertos_621710_102.html

Rodríguez Samudio, R. E. (2019). La privacidad en las ciudades inteligentes. *Revista CES Derecho, 10*(2), 641-653. https://revistas.ces.edu.co/index.php/derecho/article/view/5205

Sanabria González, M. (s.f.). *Análisis de la privacidad en las redes sociales* (Trabajo fin de grado). Universidad de Extremadura. http://dehesa.unex.es/bitstream/handle/10662/6606/TFGUEX_2017_Sanabria_Gonzalez.pdf?sequence=1&isAllowed=y

Sofistic Cybersecurity. (27 de diciembre de 2019). *6 tendencias en ciberseguridad para 2020.* https://www.sofistic.com/blog-ciberseguridad/tendencias-ciberseguridad-2020/

Tyco Seguridad. (14 de enero de 2020). *Ciberataques en 2020: las nuevas amenazas en seguridad informática.* https://blogseguridad.tyco.es/noticias/ciberataques-en-2020-las-nuevas-amenazas-en-seguridad-informatica/