Unidad 11: PRIVACIDAD

BLOQUE III – Redes e Internet

CONTENIDOS

1. Conceptos básicos.
2. Relación entre privacidad y seguridad.
3. Privacidad desde el diseño y en el despliegue.

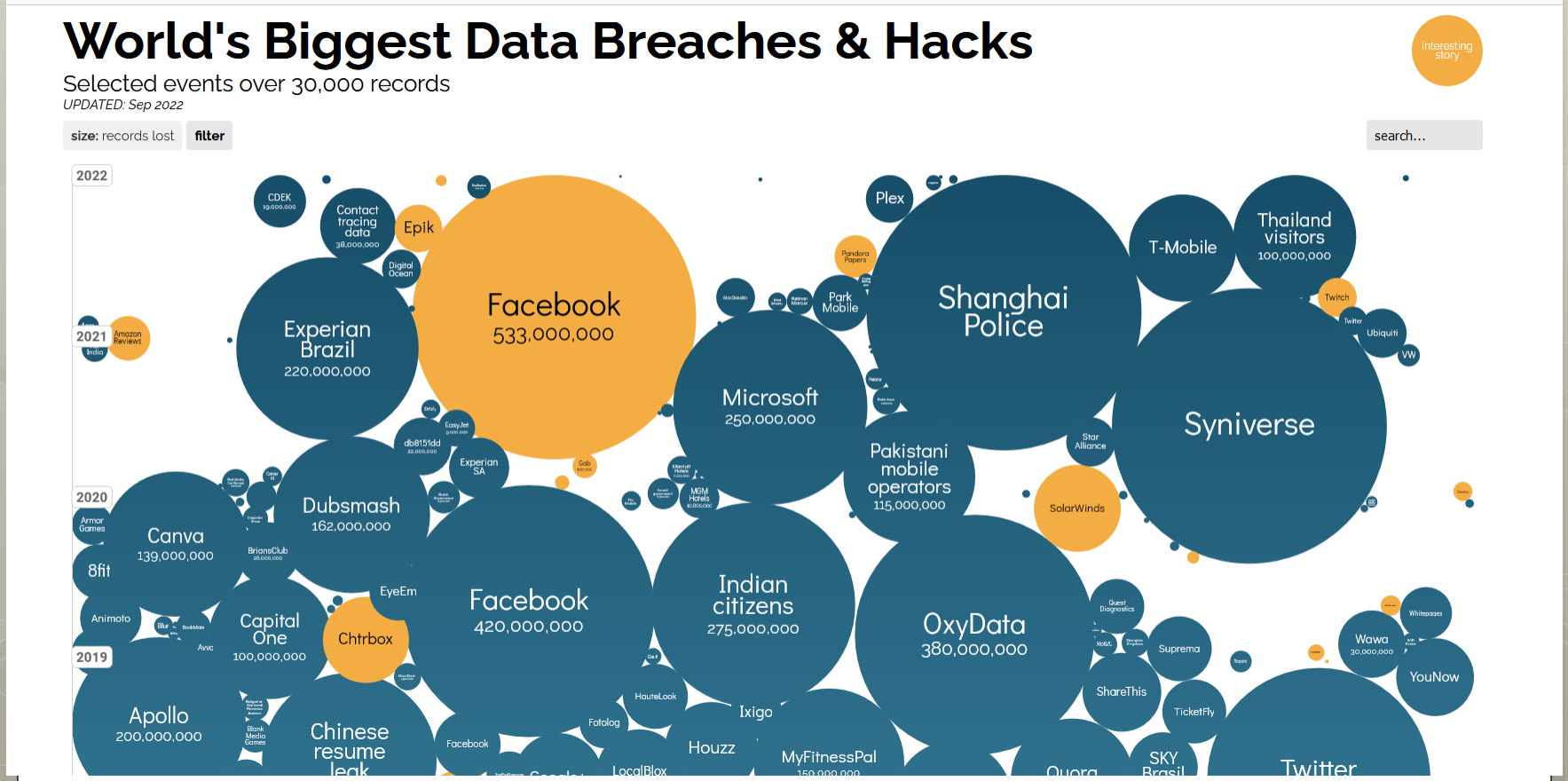
1. Conceptos básicos

- Se define la Privacidad como **"el ámbito de la vida personal de un individuo, quien se desarrolla en un espacio reservado, el cual tiene como propósito principal mantenerse confidencial"**.
- Intimidad y protección de datos son conceptos relacionados pero no son sinónimos.
  - Las compañías y personas jurídicas tienen derecho a la privacidad, pero no a la intimidad, que se considera un derecho humano.
  - La protección de datos es el medio por el cual conseguimos privacidad, tiene que ver con la seguridad.

De las pequeñas fugas…..


….. a las grandes brechas

https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



1. Conceptos básicos

- Ya hemos hablado en la asignatura de las brechas de datos.
  - Pero no es lo mismo que se pierdan en una brecha los presupuestos de una empresa que el historial médico de una persona.
  - Los datos suelen clasificarse según su nivel de sensibilidad y de los impactos que su revelación podrían llegar a provocar.
- Los datos personales son cualquier información relativa a una persona física viva identificada o identificable.
- La información de identificación personal (PII) es cualquier dato que pueda identificar a una persona específica, como el nombre, el número de identificación emitido por el gobierno, la fecha de nacimiento o su email.

1. Conceptos básicos

- Desde el punto de vista de los impactos para las personas, según el NIST, las amenazas a la privacidad (no sólo las brechas) pueden provocar:

Appropriation: Personal information is used in ways that exceed an individual's expectation or authorization. Appropriation occurs when personal information is used in ways that an individual would object to or would have expected additional value for, absent an information asymmetry or other marketplace failure. Privacy harms that Appropriation can lead to include loss of trust, economic loss or power imbalance.

Distortion: The use or dissemination of inaccurate or misleadingly incomplete personal information. Distortion can present users in an inaccurate, unflattering or disparaging manner, opening the door for discrimination harms or loss of liberty.

Induced Disclosure: Pressure to divulge personal information. Induced disclosure can occur when users feel compelled to provide information disproportionate to the purpose or outcome of the transaction. Induced disclosure can include leveraging access or privilege to an essential (or perceived essential) service. It can lead to harms such as power imbalance or loss of autonomy.

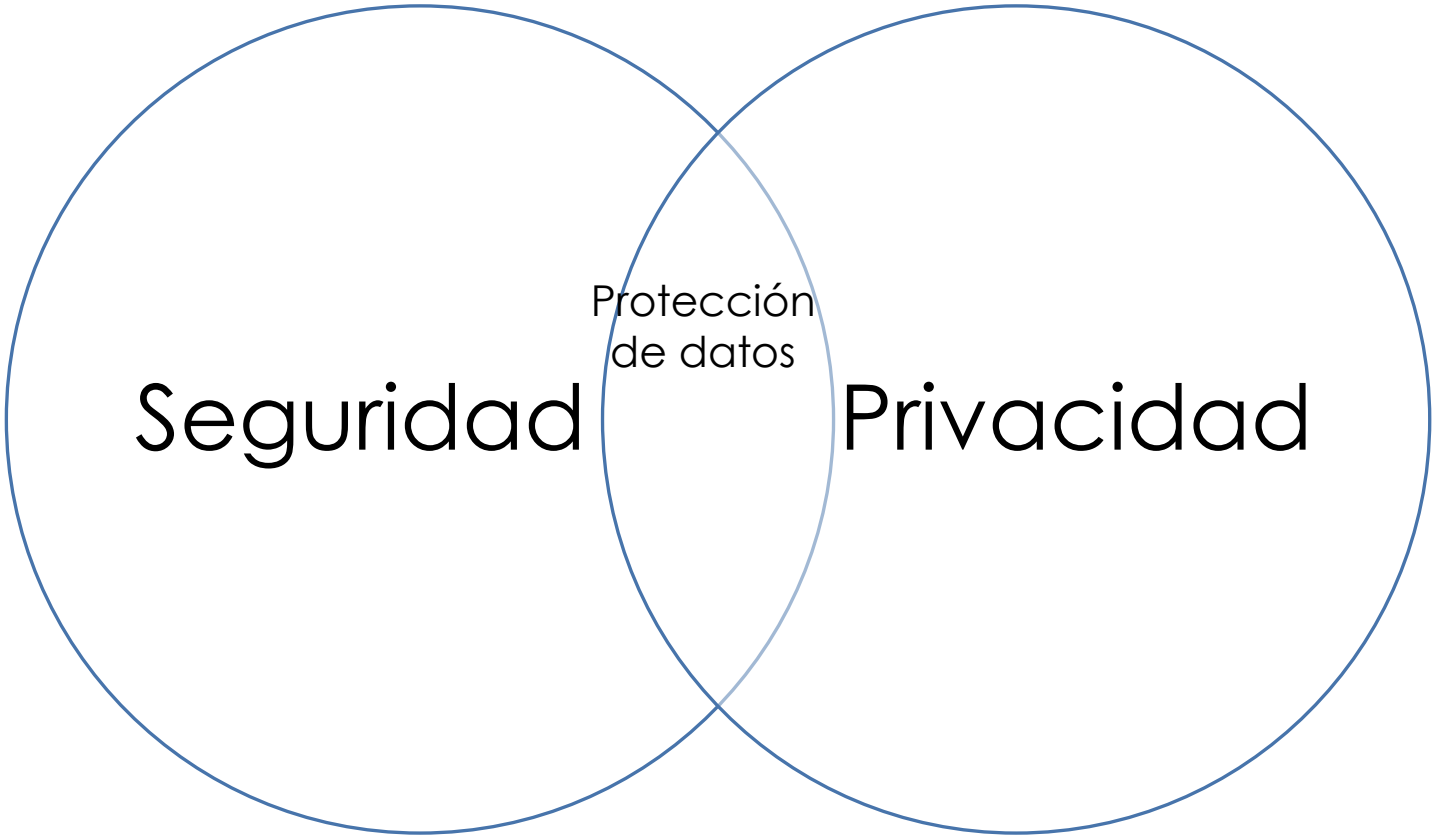
Insecurity: Lapses in data security. Lapses in data security can result in a loss of trust, as well as exposing individuals to economic loss, and stigmatization.

Surveillance: Tracking or monitoring of personal information that is disproportionate to the purpose or outcome of the service. The difference between the data action of monitoring and the problematic data action of surveillance can be very narrow. Tracking user behavior, transactions or personal information may be conducted for operational purposes such as protection from cyber threats or to provide better services, but it becomes surveillance when it leads to harms such as power imbalance, loss of trust or loss of autonomy or liberty.

Unanticipated Revelation: Non-contextual use of data reveals or exposes an individual or facets of an individual in unexpected ways. Unanticipated revelation can arise from aggregation and analysis of large and/or diverse data sets. Unanticipated revelation can give rise to stigmatization, power imbalance and loss of trust and autonomy.

Unwarranted Restriction: Unwarranted restriction to personal information includes not only blocking tangible access to personal information, but also limiting awareness of the existence of the information within the system or the uses of such information. Such restriction of access to systems or personal information stored within that system can result in harms such as exclusion, economic loss and loss of trust.

2. Relación entre privacidad y seguridad



2. Relación entre privacidad y seguridad

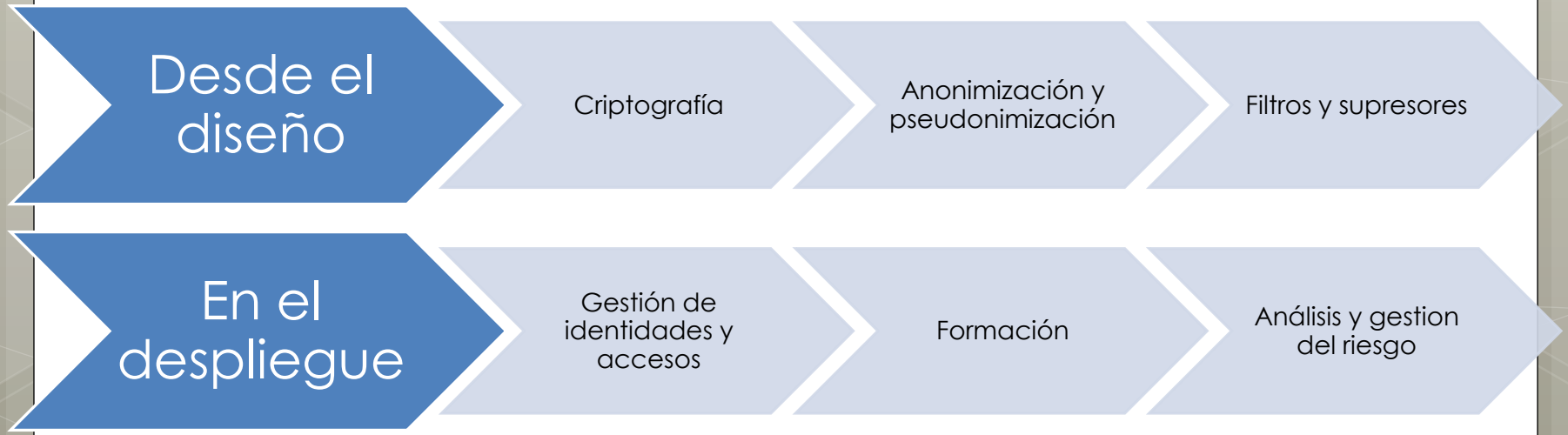
- La seguridad nos permite proteger los datos, su confidencialidad.
- Pero la privacidad es mucho más.
  - Para empezar, no recoge sólo aspectos tecnológicos, sino también humanos, éticos, políticos, económicos, legales.
- Sin en ciberseguridad se suelen encontrar equipos multidisciplinares prácticamente en todas las organizaciones, en privacidad es aún más importante.

2. Relación entre privacidad y seguridad

- Preocupan especialmente las siguientes amenazas:
  - El gran número de agentes involucrados en el tratamiento de datos.
  - El alto grado de externalización (no se sabe en manos de quién están los datos en muchas ocasiones)..
  - La falta de concienciación de todos estos agentes.
  - El uso de dispositivos móviles y de sensores muy heterogéneos y distribuidos.
  - La lentitud de las normativas y regulaciones en comparación con los avances tecnológicos.
  - La mala adaptación que en ocasiones se hace de las soluciones tradicionales a los nuevos paradigmas.

3. Privacidad desde el diseño y en el despliegue

- Recordad siempre que lo básico es:



3. Privacidad desde el diseño y en el despliegue

- Pero además, hay que tener en cuenta otros aspectos en la frontera con la seguridad:
  - ¿Qué ocurre con las vulnerabilidades de la infraestructura y de la red? MitM, secuestros de sesión, denegaciones de servicio, infecciones por malware.
  - ¿Y con las debilidades de las aplicaciones y las APIs? Inyecciones de código y comandos, desbordamientos, forgeries.
  - ¿Con las pérdidas o robos de dispositivos? Daño físico.
  - ¿Con los usuarios poco concienciados? Ingeniería social.

3. Privacidad desde el diseño y en el despliegue

- Segmentación de redes (firewalls, vLANs, DMZs, diodos de datos)
- Protección del perímetro (firewall DPI, whitelisting, IDPS, NAC, DLP)
- Uso de protocolos de comunicaciones seguros (IPSec, TLS)
- VPNs seguras
- Redes inalámbricas seguras

3. Privacidad desde el diseño y en el despliegue

- Codificación segura
- Ciclo de vida seguro
- APIs seguras
- Uso de Trusted Operating Systems
- SO y aplicaciones actualizados a su última versión

3. Privacidad desde el diseño y en el despliegue

Definición y comunicación de políticas

Insider Threat Program (ITP)

Papel del CSO o del CISO (y del DPD ó DPO)

Para practicar un poco

1. Prueba la herramienta https://haveibeenpwned.com/ para saber si tus datos se han visto involucrados en alguna brecha de datos.
2. Echa un vistazo al blog de la Agencia Española de Protección de Datos y a sus últimas publicaciones: https://www.aepd.es/es/prensa-y-comunicacion/blog (y en general, a todos los recursos, guías y publicaciones que tienen en su web).
3. Investiga sobre los denominados patrones oscuros (o *dark patterns*) y sobre el concepto de la economía de la vigilancia.

Referencias

- Fotografías
  - https://unsplash.com
- Iconos
  - https://www.flaticon.es/

Reconocimiento-CompartirIgual 3.0 España (CC BY-SA 3.0 ES)

©2019-2022 Marta Beltrán URJC (marta.beltran@urjc.es)
Algunos derechos reservados.
Este documento se distribuye bajo la licencia “Reconocimiento-CompartirIgual 3.0 España” de Creative Commons, disponible en **https://creativecommons.org/licenses/by-sa/3.0/es/**