Ciberseguridad y uso responsable de la red

JUNTA DE EXTREMADURA

@crepresa

LinkedIn.com/in/crepresa

Carlos Represa Estrada

carlos.represa@grupo-ae.com

tfno 691654490

https://www.grupo-ae.com/beonlinebyHP/

http://reinventtheclassroom.com/

El objetivo de la jornada de hoy será el acercamiento al concepto de ciberseguridad y a los nuevos riesgos derivados del teletrabajo y las oficinas virtuales en el entorno del RGPD mediante experiencias prácticas realizadas e entornos de navegación real

1.- ¿Qué es un encargado del tratamiento y cuál es su función principal?

El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio al responsable que conlleva el tratamiento de datos personales por cuenta de éste.

2.- ¿Qué tratamientos puede llevar a cabo un encargado sobre los datos que le han sido encomendados?

El encargado puede realizar todos los tratamientos, automatizados o no, que el responsable del tratamiento le haya encomendado formalmente. La definición de tratamiento nos permite concretarlos atendiendo al ciclo de vida de la información: recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

En todo caso, deben quedar claramente delimitados en el acuerdo que se adopte.

3.- ¿Qué nivel de decisión puede asumir un encargado del tratamiento?

El encargado del tratamiento puede adoptar todas las decisiones organizativas y operacionales necesarias para la prestación del servicio que tenga contratado. En ningún caso puede variar las finalidades y los usos de los datos ni los puede utilizar para sus propias finalidades.

Las decisiones que adopte deben respetar en todo caso las instrucciones dadas por el responsable del tratamiento.

Artículo 32: Seguridad del tratamiento

1.*Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar* ***un nivel de seguridad adecuado al riesgo***

En consecuencia, a partir de mayo de 2018 los responsables y encargados de tratamiento deberán realizar su propio análisis de riesgo y evaluar qué medidas de seguridad técnicas y organizativas consideran que deben de ser aplicables para garantizar la seguridad y confidencialidad en el tratamiento de datos personales

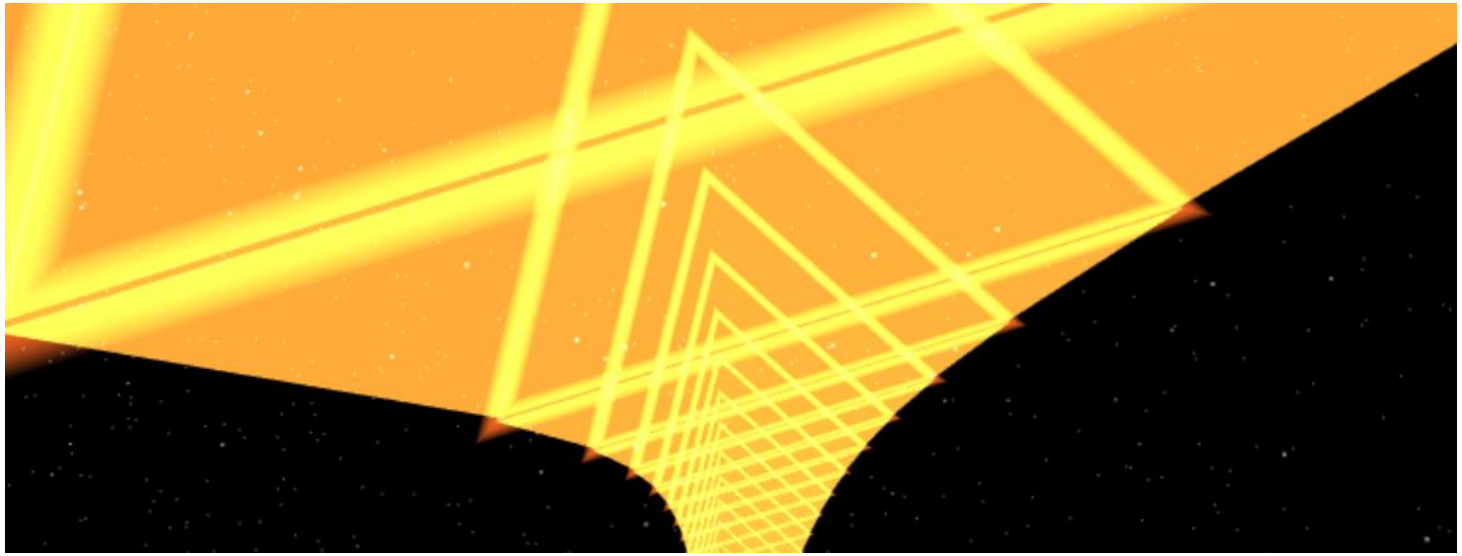
Disposición adicional vigesimotercera Datos personales de los alumnos

1. Los centros docentes podrán recabar los datos personales de su alumnado que sean necesarios para el ejercicio de su función educativa. Dichos datos podrán hacer referencia al origen y ambiente familiar y social, a características o condiciones personales, al desarrollo y resultados de su escolarización, así como a aquellas otras circunstancias cuyo conocimiento sea necesario para la educación y orientación de los alumnos.

2. Los padres o tutores y los propios alumnos deberán colaborar en la obtención de la información a la que hace referencia este artículo. La incorporación de un alumno a un centro docente supondrá el consentimiento para el tratamiento de sus datos y, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad, en los términos establecidos en la legislación sobre protección de datos. En todo caso, la información a la que se refiere este apartado será la estrictamente necesaria para la función docente y orientadora, no pudiendo tratarse con fines diferentes del educativo sin consentimiento expreso.

3. En el tratamiento de los datos del alumnado se aplicarán normas técnicas y organizativas que garanticen su seguridad y confidencialidad. El profesorado y el resto del personal que, en el ejercicio de sus funciones, acceda a datos personales y familiares o que afecten al honor e intimidad de los menores o sus familias quedará sujeto al deber de sigilo.

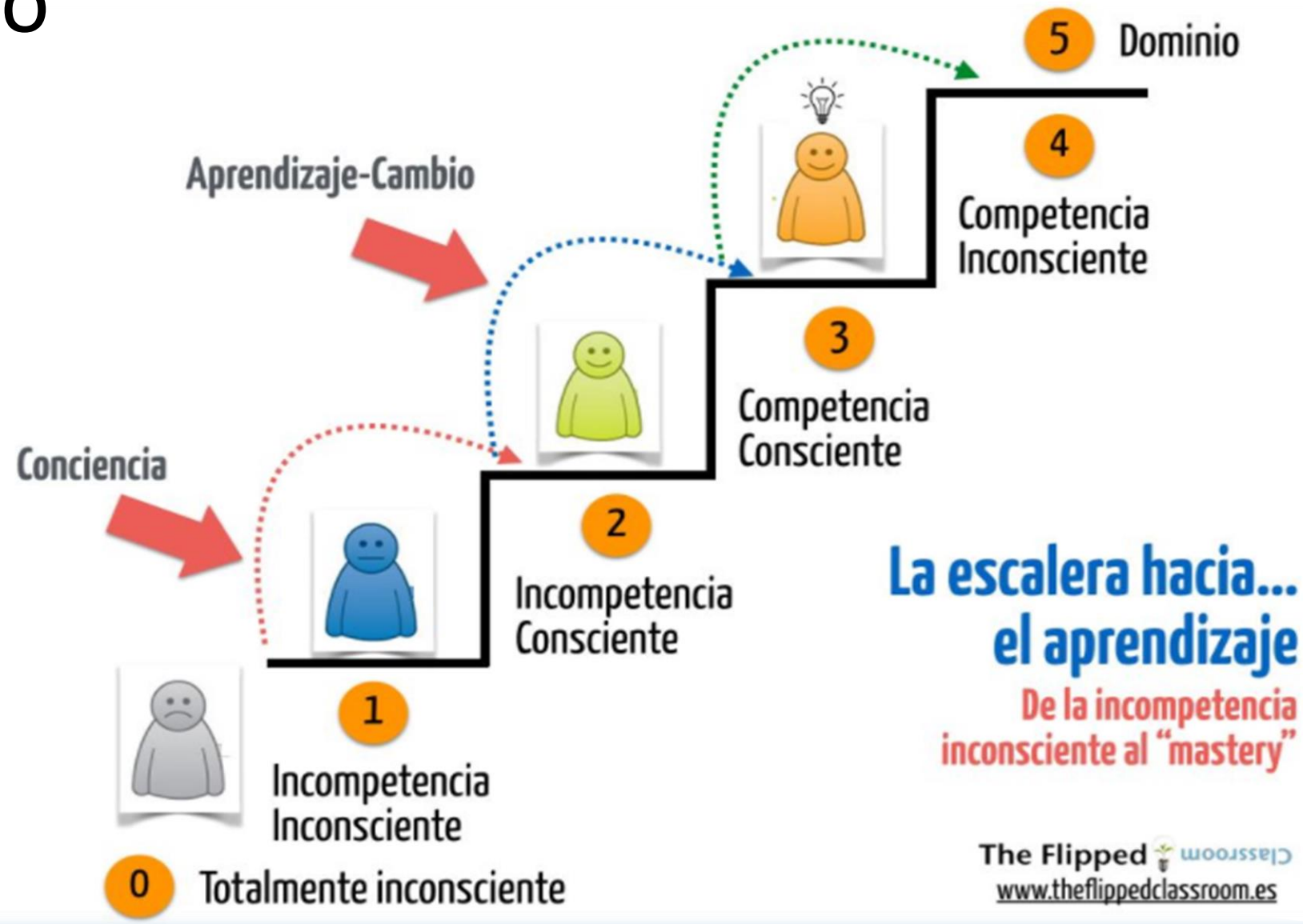
LA CIBERSEGURIDAD



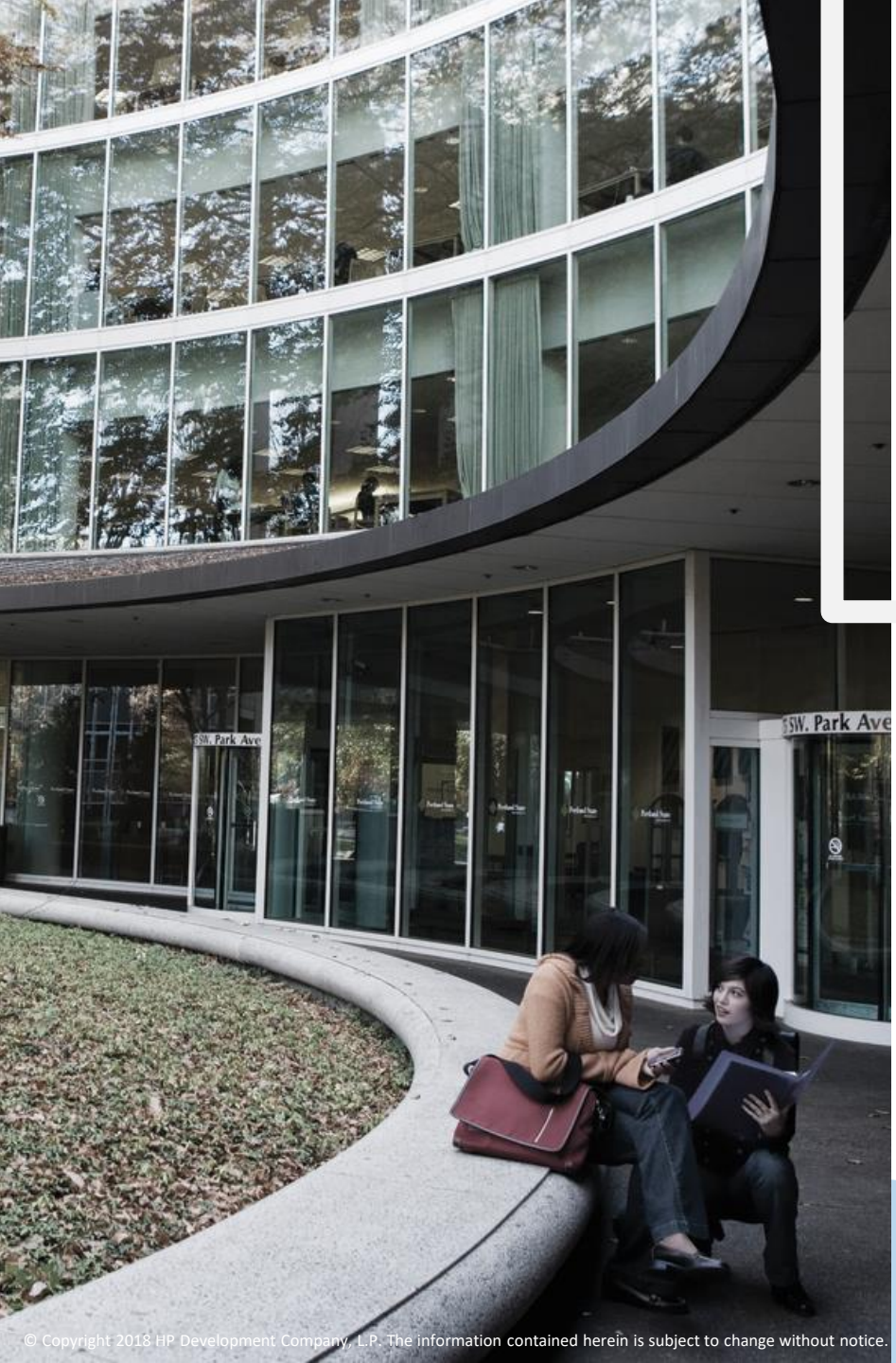
https://cybermap.kaspersky.com/es


Security
Safety

“El Conocimiento Es Un Antidoto Para El Riesgo”



Ejemplo de competencia inconsciente:



Regardless of the part of the PC an attack targets, or how it works,

EL NAVEGADOR ES EL VECTOR #1 DE INFECCIÓN

81%

están de acuerdo en que el navegador web inseguro es el principal vector de ataque[2]

Ponemon Institute, patrocinado por Spikes Security "The Challenge of Preventing Browser-Borne Malware", febrero de 2015

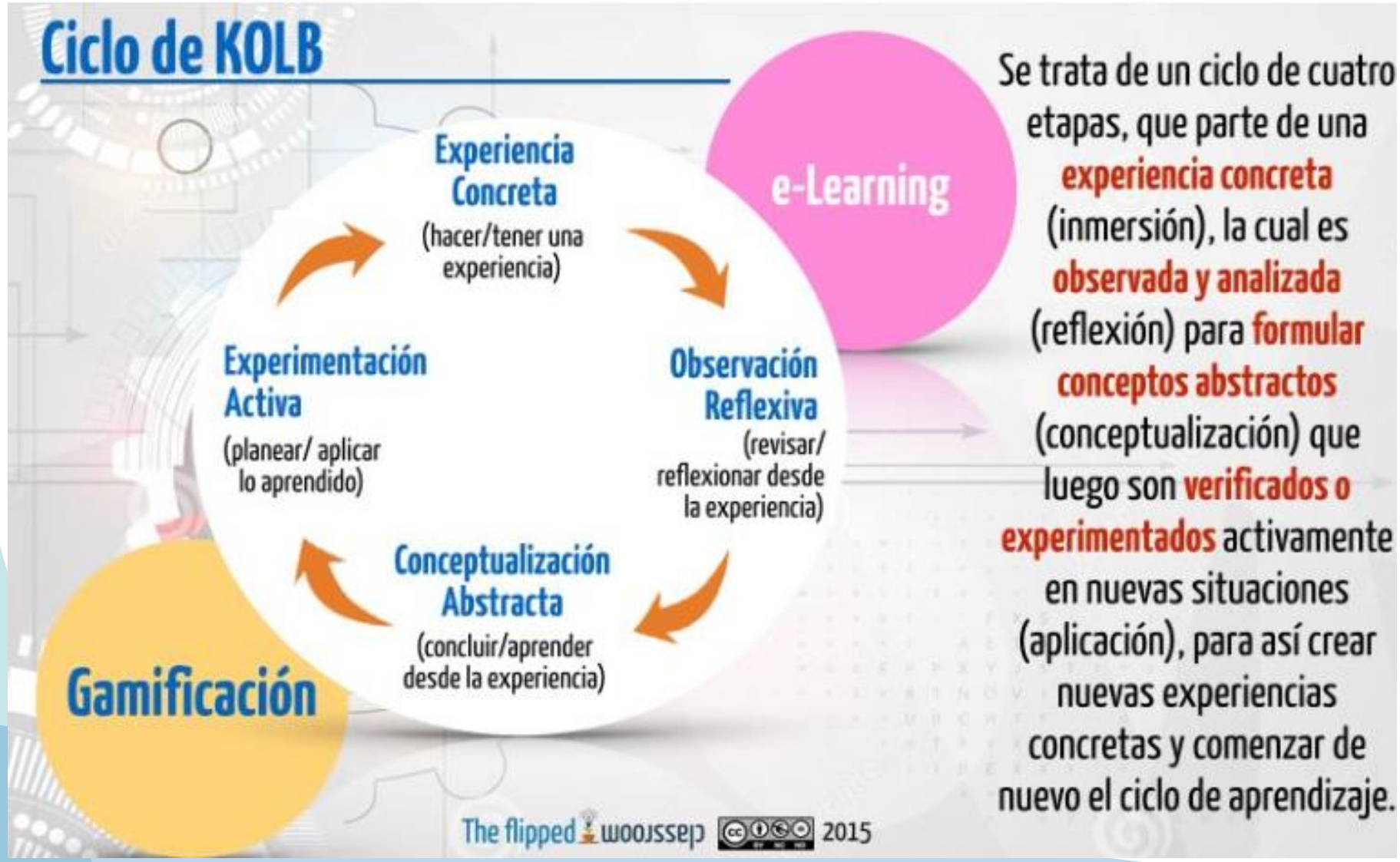
48%

no tienen un programa de capacitación de concienciación sobre la seguridad de los empleados[3]

PWC "Fortalecimiento de la sociedad digital contra los shocks cibernéticos: hallazgos clave de la Encuesta global de ® de seguridad de la información 2018"

¿ Que bienes protege la Seguridad + Privacidad?

PROPUESTA


Ciclo de KOLB
Experiencia Concreta
(hacer/tener una experiencia)
Observación Reflexiva
(revisar/ reflexionar desde la experiencia)
Conceptualización Abstracta
(concluir/aprender desde la experiencia)
Experimentación Activa
(planear/ aplicar lo aprendido)
e-Learning
Gamificación
Se trata de un ciclo de cuatro etapas, que parte de una experiencia concreta (inmersión), la cual es observada y analizada (reflexión) para formular conceptos abstractos (conceptualización) que luego son verificados o experimentados activamente en nuevas situaciones (aplicación), para así crear nuevas experiencias concretas y comenzar de nuevo el ciclo de aprendizaje.
The flipped classroom
2015

TALLERES

Alfabetización informacional

“ Los operadores de google”

- Protección de derechos fundamentales
- Seguridad de la identidad en RRSS
- Hacking google

Reputación digital

“La importancia de la imagen ”

- ¿ que es una imagen en la red?
- ¿ que son los metadatos?

Reputación digital

"Del egosurfing al derecho al olvido"

- ¿ que es la transparencia en la red?
- ¿ La red olvida?

El IoD

"El ataque de las neveras asesinas"

- Eso a mi no me puede pasar
- Mi impresora va por libre

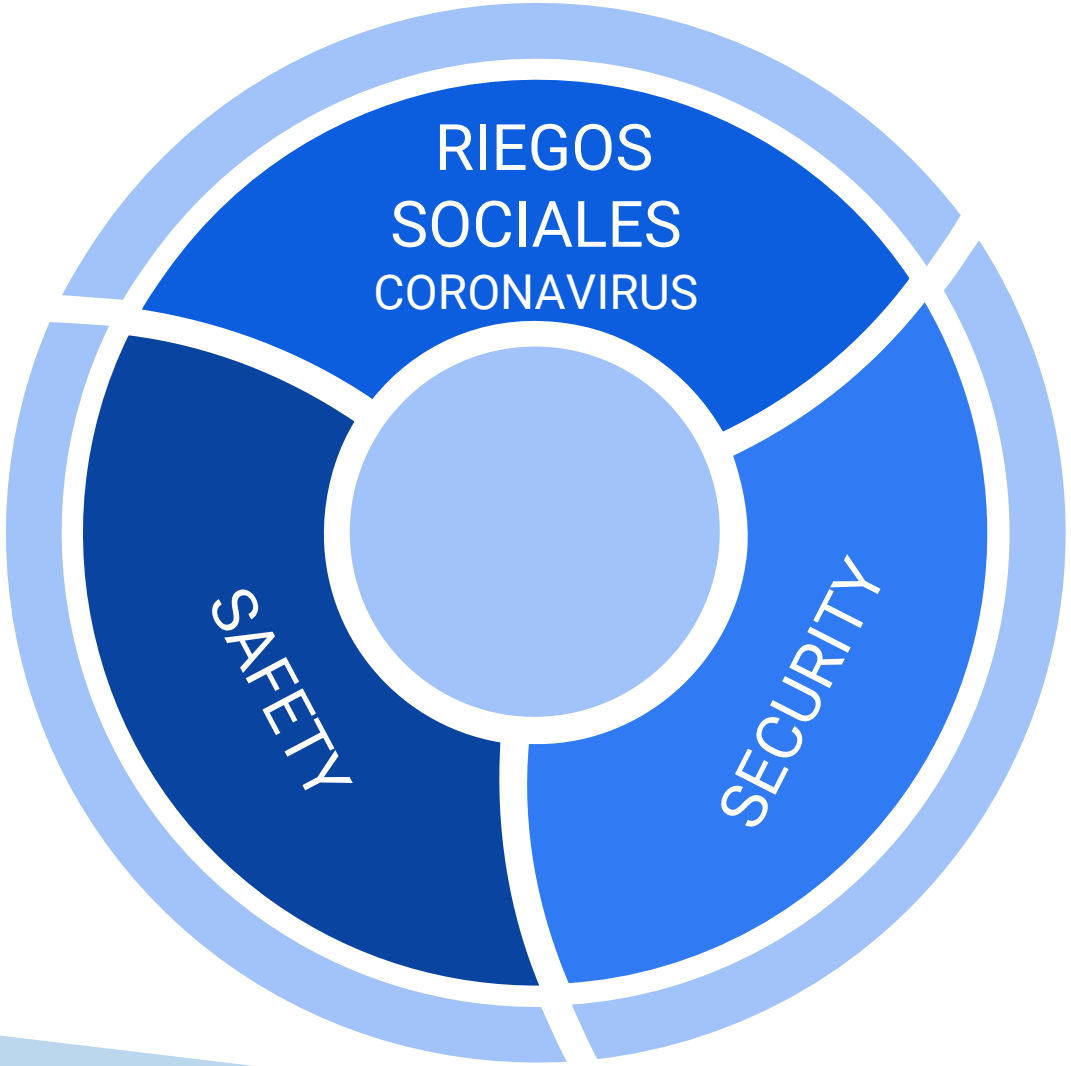
…Hay más virus detras de #Covid19…

"Es que este mail es de mi jefe cariño"

- Del rogue software al ramsonware
- Pues no, no era el jefe

¿Es verdad lo de la pornografía infantil en la red?

INDICE



1- RIESGOS SOCIALES DIGITALES

- BULOS / CORONABULOS: FAKE NEWS

2- SEGURIDAD TÉCNICA E INFORMÁTICA. SECURITY

- DEL PHISING AL CORONAPHISING
- PHARMING
- RAMSONWARE

3- PRIVACIDAD Y PROTECCIÓN DE DATOS. SAFETY

- IDENTIDAD DIGITAL

1- RIESGOS SOCIALES DIGITALES

BULOS / CORONABULOS

http://gg.gg/gyeok

FINALIDADES

1- Perjudicar la imagen de una persona / grupo / partido etc

2- Analizar difusión y seguidores mediante perfiles (profiling)

3- Crear alarma social

4- Crear estado de opinión

BENEFICIOS PARA LOS AUTORES

- **El ego 2.0 (el gamberro digital)**
- **El beneficio económico del clic**
- **Desestabilización política (el gran hackeo)**
- **Desestabilización económica**

DECÁLOGO DE RECOMENDACIONES

1. **Cuestionar siempre lo que llega por redes sociales si el contenido está relacionado con el coronavirus.**
2. **No compartir nada si no se está 100% seguro de si es verdad.**
3. **No confiar en los videos y audios de procedencia no clara, incluso en los grupos de familiares y amigos cercanos**

5. Los titulares alarmistas. En una situación como la actual es especialmente grave contribuir a generar alarma social injustificada.

6. No atender nunca las informaciones que nos piden datos personales, número de teléfono, etc. Pueden ser un engaño

6. Las recomendaciones médicas o sanitarias que no vengan de una fuente oficial. No hay que darles credibilidad ni difundirlas.

Ejemplo de fuentes oficiales:

- Ministerio de Sanidad
- Organización Mundial de la Salud
- Policía Nacional y Guardia Civil
- Consejerías autonómicas de Salud y servicios oficiales de emergencias

7. Comprobar que el texto dice lo mismo que el titular. A veces el titular pretende captar nuestra atención, pero luego no se corresponde con lo que se dice en el cuerpo de la noticia.

8. Si no se está seguro, recordad: no compartáis

+ Información

https://www.newtral.es/

https://www.newtral.es/guia-sobre-bulos-para-padres-y-madres/20200323/

https://maldita.es/malditobulo/

2- SEGURIDAD TÉCNICA E INFORMÁTICA.

SECURITY

- DEL PHISING al CORONAPHISING

ORIGEN

MAYOR VULNERABILIDAD Y NECESIDAD DE INFORMACIÓN

CONCEPTO

Método utilizado por los ciberdelincuentes para, de forma fraudulenta, obtener información confidencial de su víctima relativa a sus datos personales, claves de acceso, cuentas bancarias, números de tarjeta de crédito, identidades, etc. ***para luego ser usados de forma fraudulenta con el fin de suplantar la identidad de la víctima.***

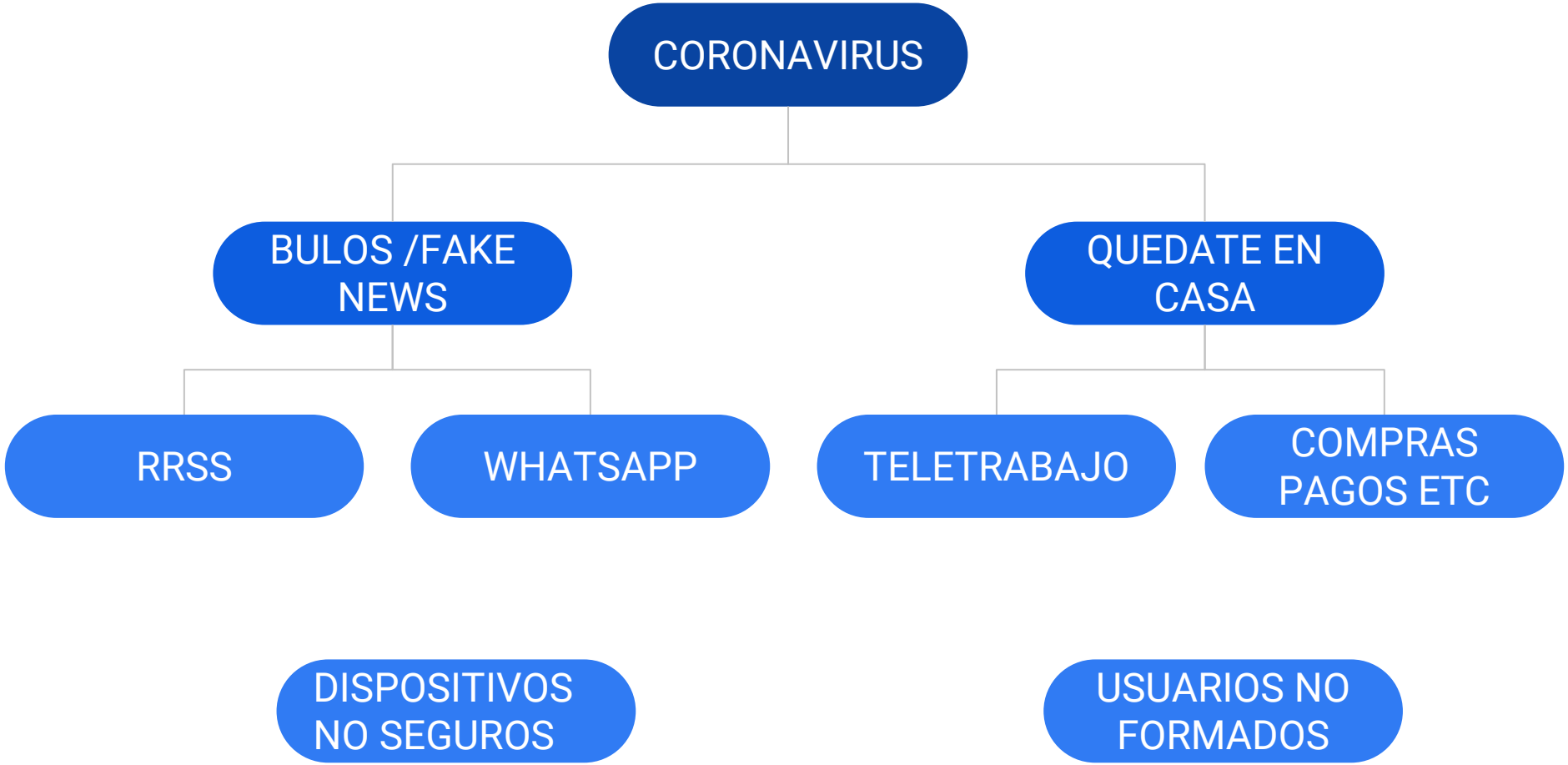
PHARMING

- Manipulación de nombres de dominio normalmente producido por un código malicioso, que permite que el usuario cuando introduce la dirección de una página web, se le conduzca en realidad a otra falsa, que simula ser la deseada.
- Enlace a webs aparentemente legales con técnicas de phising, mensajería, whatsapp etc

RAMSONWARE

Software malicioso que infecta el ordenador y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema.Se puede instalar a través de enlaces engañosos o archivos adjuntos incluidos en un mensaje de correo electrónico, mensaje instantáneo o sitio web. El ransomware tiene la **capacidad de bloquear la pantalla del dispositivo o cifrar archivos importantes con una contraseña**.

.....ESTÁ PASANDO.....



.....ESTÁ PASANDO.....

Edición impresa

Qué!

Qué! Radio

QUÉ! ACTUALIDAD | QUÉ! DEPORTES | QUÉ! TV | QUÉ! FAMOSOS | QUÉ! CURIOSAS | QUÉ! CIUDADES | QUÉ! ESTILO DE VIDA | + QUÉ!

Inicio › sociedad

Esta falsa app del coronavirus bloquea tu smartphone y pide un rescate

17 marzo, 2020

LA CRISIS DEL CORONAVIRUS >

Interior alerta de una quincena de ciberestafas que utilizan como señuelo el coronavirus

Los expertos policiales destacan la peligrosidad de una web que ofrece falsos diagnósticos de la enfermedad

6

ÓSCAR LÓPEZ-FONSECA | JORDI PÉREZ COLOMÉ

Madrid - 23 MAR 2020 - 01:41 CET

.....ESTÁ PASANDO.....

- *spams* / envíos masivos de correos electrónicos
- emails falsos con adjuntos maliciosos, *ransomware*
- e-shops tiendas virtuales que son un fraude
- apps maliciosas

……Y ACABA DE PASAR ……

LA CRISIS DEL CORONAVIRUS >

La policía detecta un ciberataque al sistema informático de los hospitales

Los autores pretendían inutilizar los ordenadores por medio de correos electrónicos enviados al personal sanitario

RECOMENDACIONES DE SEGURIDAD

1. Actualiza el sistema y pon al día tu antivirus.Pero en TODOS los dispositivos, especialmente **Smartphones.**

1. Realiza todas las actualizaciones que tengas pendientes y haz una revisión con el antivirus, estarás creando una barrera más fuerte contra posibles amenazas.

Visita www.osi.es

3. Extrema la precaución al usar memorias USB o descargar archivos. No te confíes, tu espacio de trabajo contiene información de tus clientes

4. Mantén la alerta ante páginas fraudulentas, enlaces y adjuntos

5. Separa tu área personal del área de trabajo.. Procura no mezclar documentos y archivos personales con los del trabajo, creando **cuentas de usuario diferentes.**

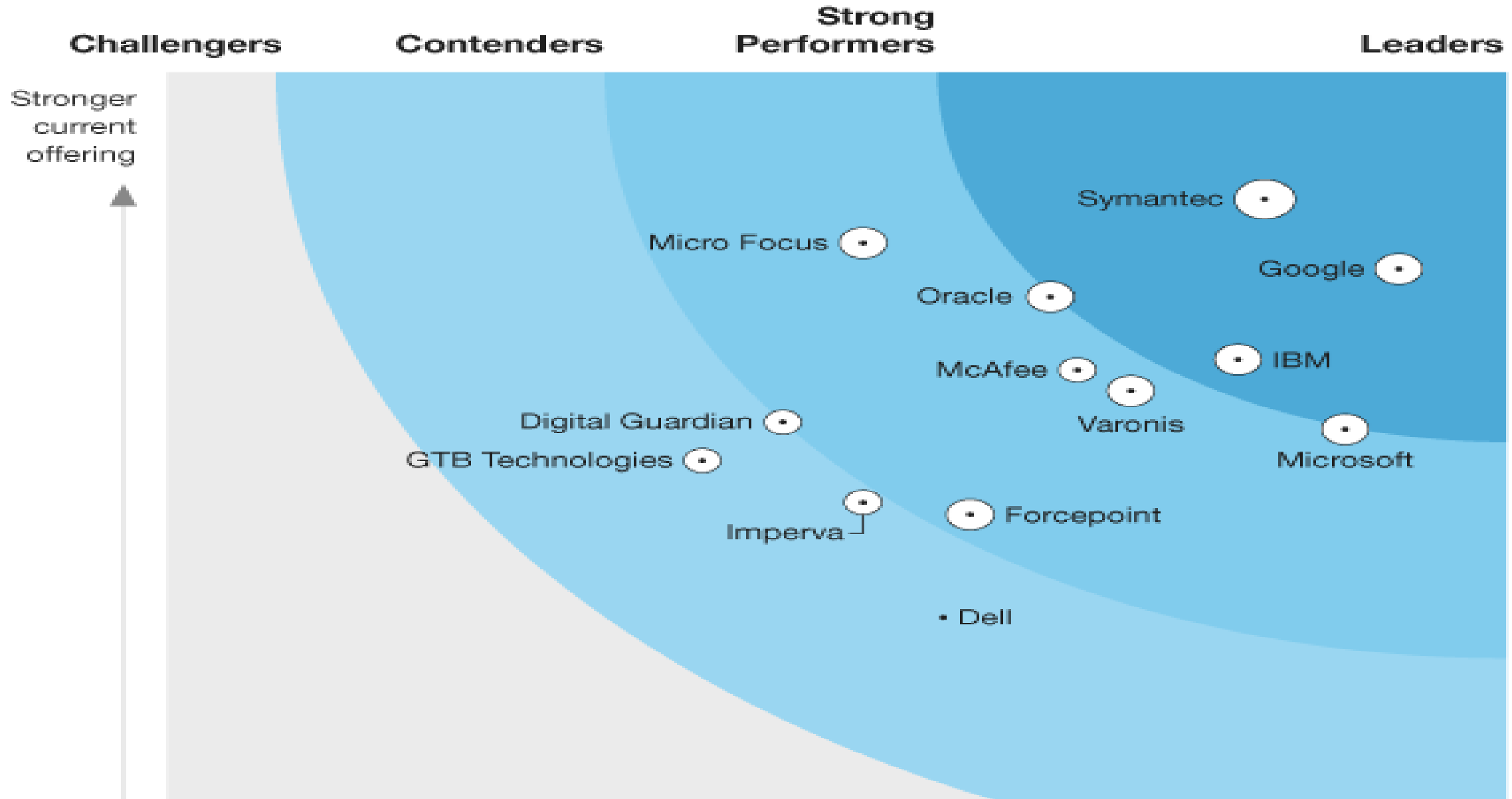
7. Utiliza herramientas adecuadas para **transferir la información** más sensible. A pesar de las circunstancias, proteger la información sensible de los menores siempre debe ser una prioridad con aplicaciones aplicaciones de gestión educativa

MAS INFORMACIÓN:
https://www.osi.es/es/cibercovid19

THE FORRESTER WAVE™

Data Security Portfolio Vendors

Q2 2019



https://discover.microsoft.com/cyber-security-assessment-to-protect-your-business/?_lrsc=42a31d99-9888-42cc-9822-edc125006531

Enlaces de Interés

https://www.youtube.com/watch?v=KSMJqloIl7w&feature=youtu.be
https://tool.geoimgr.com/
https://www.elevenpaths.com/es/tecnologia/metashield/metashield-analyzer-online/index.html
https://hipertextual.com/2015/02/que-sabe-google-sobre-ti
https://plusdireccion.es/francisco-martinez-sanchez-valdemorillo-918974369
https://offers.hubspot.es/demo-hspd?utm_id=2660752799 47&utm_medium=paid&utm_source=google&utm_term=Marketing_hubspot_ES&utm_campaign=Marketing_MQLs_ES_AdWords_LATAM_IBERIA_Brand-HubSpot_e_c_1053843554&hsa_tgt=kwd-6356688152&hsa_grp=54306822840&hsa_src=g&hsa_net=adwords&hsa_mt=e&hsa_ver=3&hsa_ad=266075279947&hsa_acc=2734776884&hsa_kw=hubspot&hsa_cam=1053843554&gclid=CjwKCAiAnfjyBRBxEiwA-EECLLbQojWApGBKmKRuUFiIizK-XRSlv5xFd40VpvZK90K77NN8eLkMfhoC27gQAvD_BwE
https://www.tic-tac-pills.com/herramientas/kahoot
https://whatismyipaddress.com/ip-lookup
https://www.xatakandroid.com/aplicaciones-android/probamos-f3-app-preguntas-respuestas-que-esta-alto-google-play

@crepresa

LinkedIn.com/in/crepresa

Carlos Represa Estrada

Business Developer

carlos.represa@grupo-ae.com

tfno 691654490

https://www.grupo-ae.com/beonlinebyHP/

http://reinventtheclassroom.com/