Ciberseguridad

asociación española de profesionales del turismo

aept

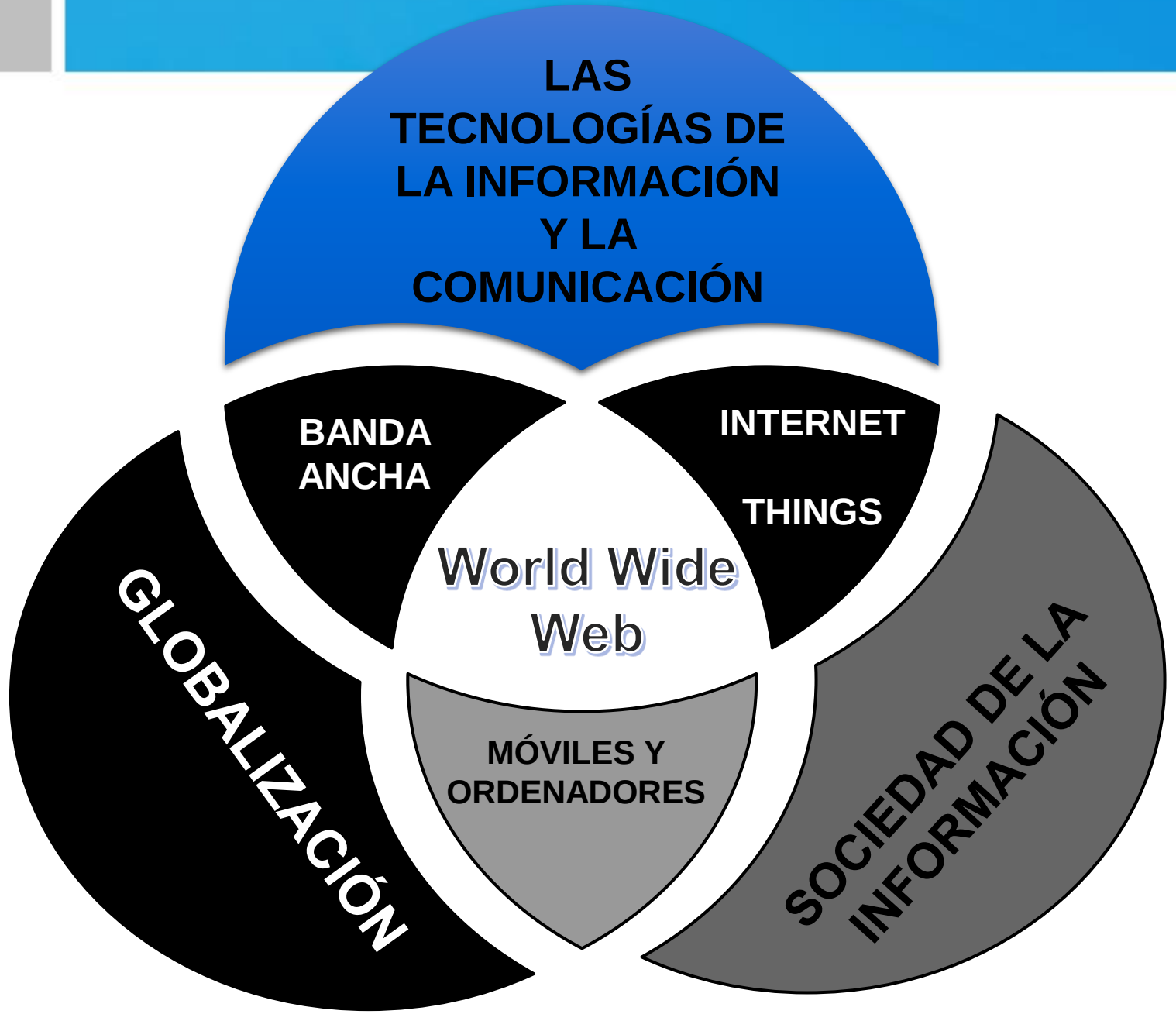
Recoletos ERD

Consultores de Seguros & Gestión de Riesgos

índice de materias

- 01. Concepto y Legislación
  - Causa de la ciberdelincuencia
  - Normativas de la Ciberseguridad

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos



Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

- La Ciberseguridad es un conjunto de herramientas y medidas de protección de los sistemas digitales

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

Causas de la ciberdelincuencia

- Económicas
- Hacktivismo
- Espionaje industrial
  - gubernamental
  - particular
- Curiosidad, afán de sembrar caos

NORMATIVAS DE LA CIBERSEGURIDAD

- **RGPD**: Responsabilidad proactiva, enfoque según riesgo desde un punto de vista europeo

- **Directiva NIS** (**S**ecurity of **N**etwork and **I**nformation **S**ystems): cooperación internacional a nivel UE. En cada país se designan CSIRTs (**C**omputer **S**ecurity **I**ncident **R**esponse **T**eams)

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

NORMATIVAS DE LA CIBERSEGURIDAD

CSIRTs EN ESPAÑA

- Entidades Públicas → **CCN** (**C**entro **C**riptográfico **N**acional)
- Particulares y Entidades Privadas → **INCIBE** (**I**nstituto **N**acional de **C**iberseguridad de **E**spaña) **(www.incibe.es)**

índice de materias

- 02. Evolución del virus a los ciberataques
  - Orígenes
  - Tipos
  - Desde 1990 hasta 2021

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

Evolución de los ciberataques

1971: CREEPER- Primer virus informático en la red ARPANET.

1982: ELK CLONER- Primer virus en Apple II

1986: BRAIN- Virús para Pc IBM

1988: Viernes 13- Elimina todos los archivos cada viernes 13

Periodo de baja implantación informática. Sobre todo tiene efecto en ámbitos militares, universitarios y de grandes empresas.

Evolución de los ciberataques

1998: CHERNOBIL- Infectó a ordenadores de todo el mundo, afectando al disco duro y al chip BIOS(Basic Input Output), localizado en la placa base, en la memoria ROM(Read Only Memory). Una vez apagado el ordenador la información sigue en la memoria.

1999: MELISSA- Difusión automática por mail.

Periodo de incremento de la implantación informática. Empieza a ser un electrodoméstico más en los hogares. Juegos, trabajos y actividades privadas. Comienza el intercambio de mail, sustituyendo a la correspondencia tradicional. Las empresas comienzan a utilizar la página web como medio de comunicación con sus clientes.

Evolución de los ciberataques

2000: I love you- A través del mail infectó a millones de ordenadores.

2007: Italian Job- Infección de más de 10.00 webs italianas. Los visitantes de las webs extendían la infección.

2009: ZEUS: Ataque a Gobiernos, grandes instituciones y grandes corporaciones.

Periodo de gran crecimiento en la implantación informática. Empieza a ser común la conectividad en las empresas y hogares por medio de WIFI. En 2007, comienza la interconexión de los terminales móviles (Blackberry y iPhone). Ecommerce y Redes Sociales empiezan su andadura.

Evolución de los ciberataques

2012: FLASHBACK- Troyano para Apple. Casi 1 millón de equipos infectados

2012: DROPBOX- Las contraseñas de más de 70 millones de usuarios se ven expuestas.

2013: CRYTOLOCKER: Primer ataque masivo de Ransomware.

2014: WIRELUCKER- Malaware para dispositivos con iOS (iPhone e iPad)

2014: WINDIGO- Servidores Linux redirigen el tráfico de 500.000 usuarios diarios a webs con malware

2015: XCODEGOSHT- La Apple Store se ve infectada por un código malicioso que infecta a más de 100 millones de usuarios.

Evolución de los ciberataques

2016: MIRAI- Caída global de internet por varias horas. Miles de millones en pérdidas.

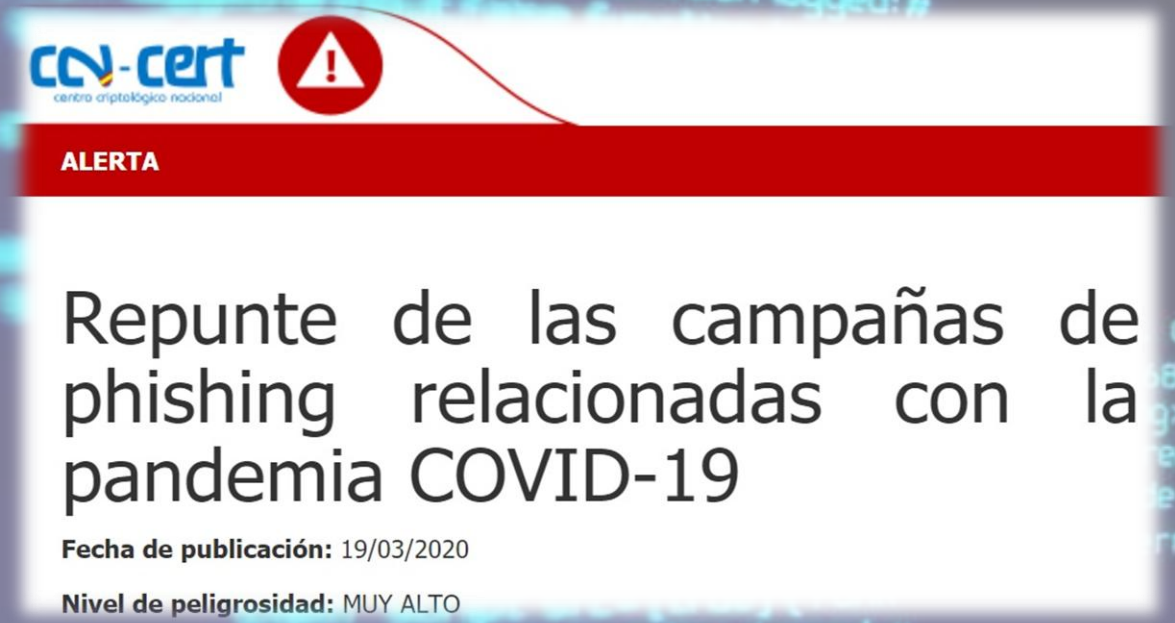
2016: HUMMINGBAD- Publicidad masiva en dispositivos Android. Más de 100 millones de terminales afectados.

2016: ACEDECEIVER: Robo de identidades en Apple.

2017: WANNACRY- Secuestro masivo de equipos informáticos en más de 150 países

En 2020 llega la pandemia de Covid-19. Las casas comparten equipos infomáticos para el desarrollo de actividades laborales y escolares. Muchas redes locales no están preparadas para esta situación inesperada y se producen ataques masivos.

EL CIBERCRIMEN SE MULTIPLICA



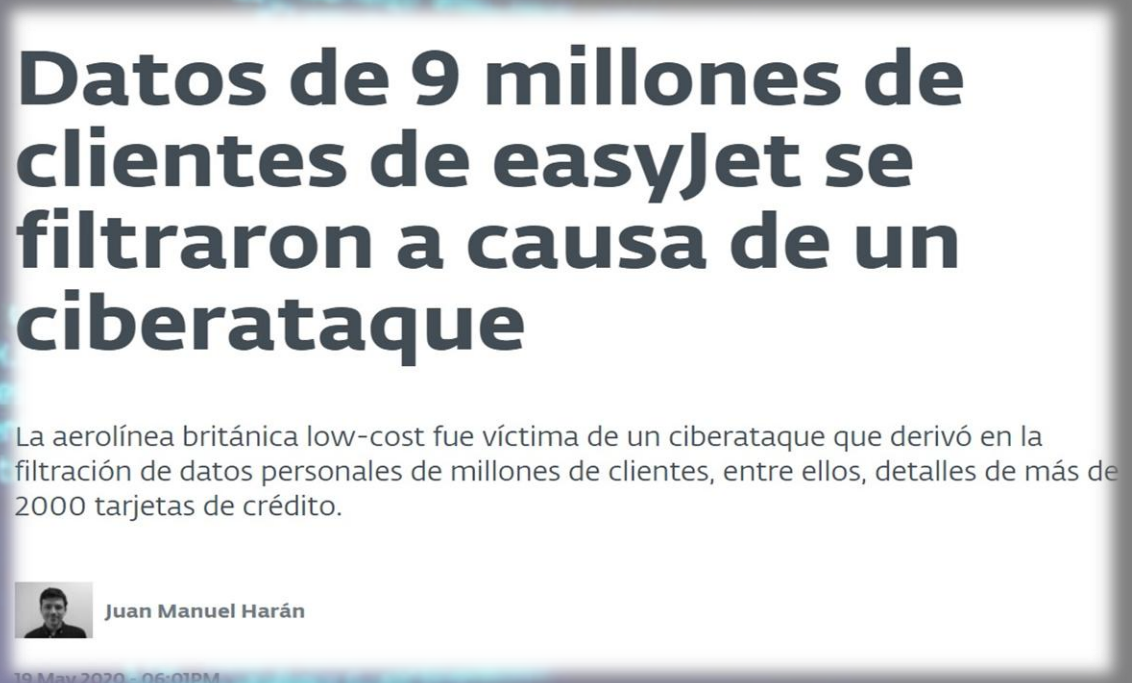
ccn-cert
centro criptológico nacional

ALERTA

Repunte de las campañas de phishing relacionadas con la pandemia COVID-19

Fecha de publicación: 19/03/2020

Nivel de peligrosidad: MUY ALTO



Datos de 9 millones de clientes de easyJet se filtraron a causa de un ciberataque

La aerolínea británica low-cost fue víctima de un ciberataque que derivó en la filtración de datos personales de millones de clientes, entre ellos, detalles de más de 2000 tarjetas de crédito.

Juan Manuel Harán

19 May 2020 - 06:01PM

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

EL CIBERCRIMEN SE MULTIPLICA

CNN | Latam | EE.UU. | Mundo | Negocios | Entretenimiento | Tecno | Deportes | Viajes | Salud | Estilo | Opinión | Video | Podcasts

EUROPA

Los ciberataques graves se duplicaron el año pasado en Europa en medio de la pandemia, según nuevas cifras

Por Nick Paton Walsh
08:21 ET(12:21 GMT) 11 Junio, 2021

Un ciberataque contra Phone House expone los datos bancarios de millones de clientes españoles

Afecta a los nombres, números de DNI, cuentas bancarias, emails, teléfonos, direcciones y fechas de nacimiento de 13 millones de clientes y trabajadores de la empresa

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

EL CIBERCRIMEN SE MULTIPLICA

PORTADA | ECONOMÍA | EMPRESAS

España sufre 40.000 ciberataques diarios: administraciones y pymes, entre los objetivos más vulnerables

Alonso Trenado • Madrid
21/06/2021 • 03:30h.

Un ciberataque a la "nube" pone en jaque a múltiples despachos profesionales

26 FEBRERO 2021

Un ciberataque a la nube pone en jaque a múltiples despachos profesionales de consecuencias incalculables

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

EL CIBERCRIMEN SE MULTIPLICA

El 'software' espía israelí Pegasus se usó en móviles de periodistas, activistas y empresarios de todo el mundo

EFE NOTICIA 19.07.2021 - 03:01H

TECNOLOGÍA

Un ciberataque tumba los servicios de varios ayuntamientos de España

El servicio en la nube ASAC ha sufrido un ciberataque que ha dejado fuera de juego a ayuntamientos como el de Oviedo y a instituciones como el Tribunal de Cuentas

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

índice de materias

- 03. Diferentes ciberataques
  - Malware
  - Inteligencia Social
  - Otros ataques

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

malware

•**VIRUS** -> Se autorreplican. Menos frecuentes hoy día. Provocan múltiples fallos de software

GUSANO -> Se autorreplican y expanden a gran velocidad. Vehículo de entrada para otras clases de malware

malware

TROYANO -> Se camuflan como software de confianza. Existen 4 tipos principales de troyanos:

- Bancario
- Backdoor/RAT
- Zombie
- Bomba de tiempo

SCAREWARE -> Bajo falsas advertencias de infección, se hace pasar por antivirus milagroso

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

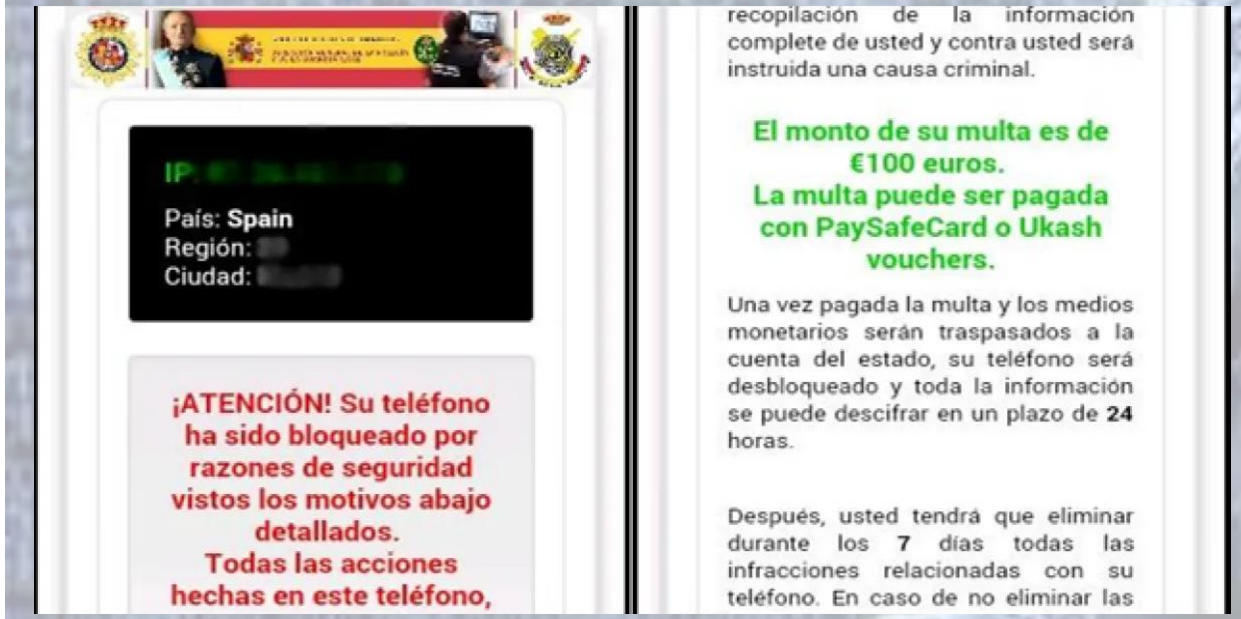
malware

CRYPTOJACKING -> Se aprovechan de ordenadores y móviles ajenos para minar criptomonedas

SPYWARE -> Keyloggers, cookies rastreadoras, spyware para móviles

- **ROOTKITS** -> Pasan inadvertidas con facilidad. Dan privilegios Root (administrador) y ocultan malware. Muy habituales en Linux

malware

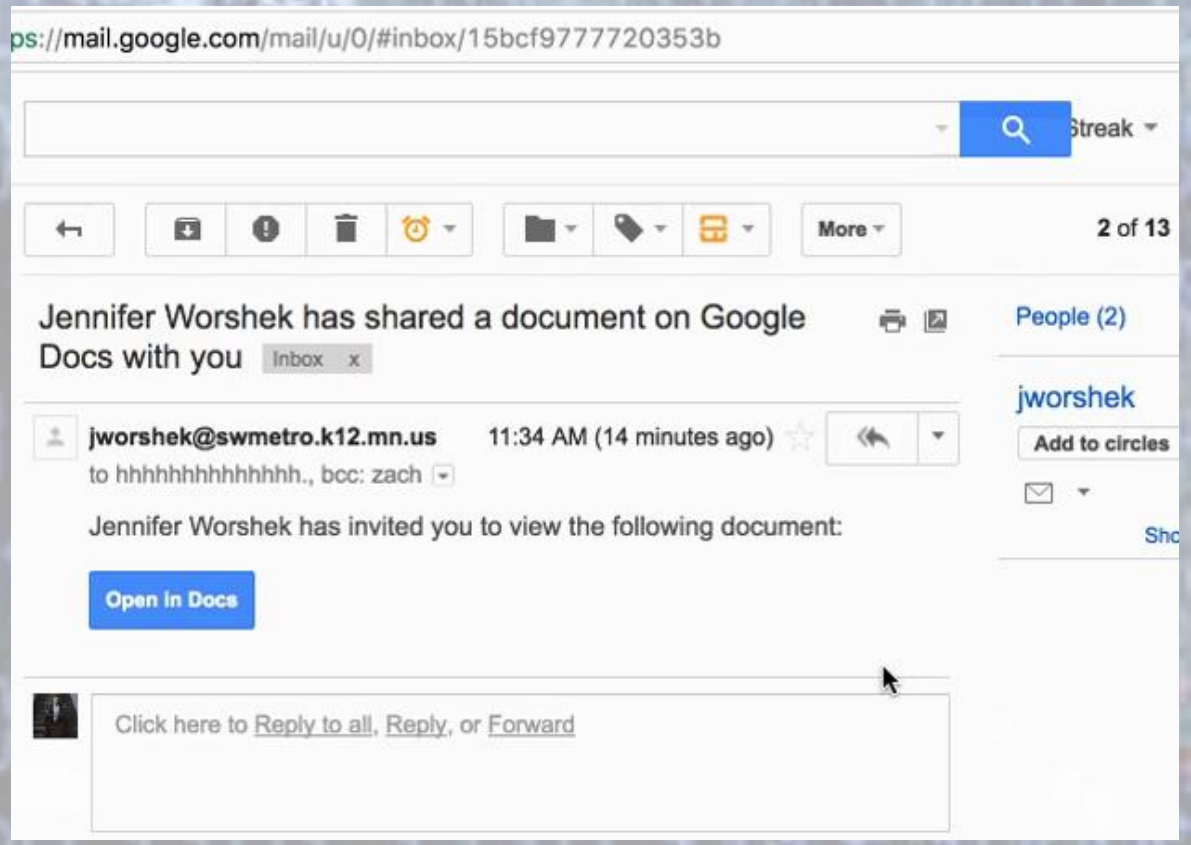


RANSOMWARE -> Encriptan la información y piden rescate en Bitcoins. Antiguamente lo pedían en Euros o Dólares Recientemente ha evolucionado a Ransomware de doble extorsión

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

Inteligencia social

- **PHISHING** -> Suplantación de identidad mediante estafas por correo, o SMS (smishing) o llamadas de voz (vishing)
- **SPEAR PHISHING** (personalizado)-> Whaling



Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

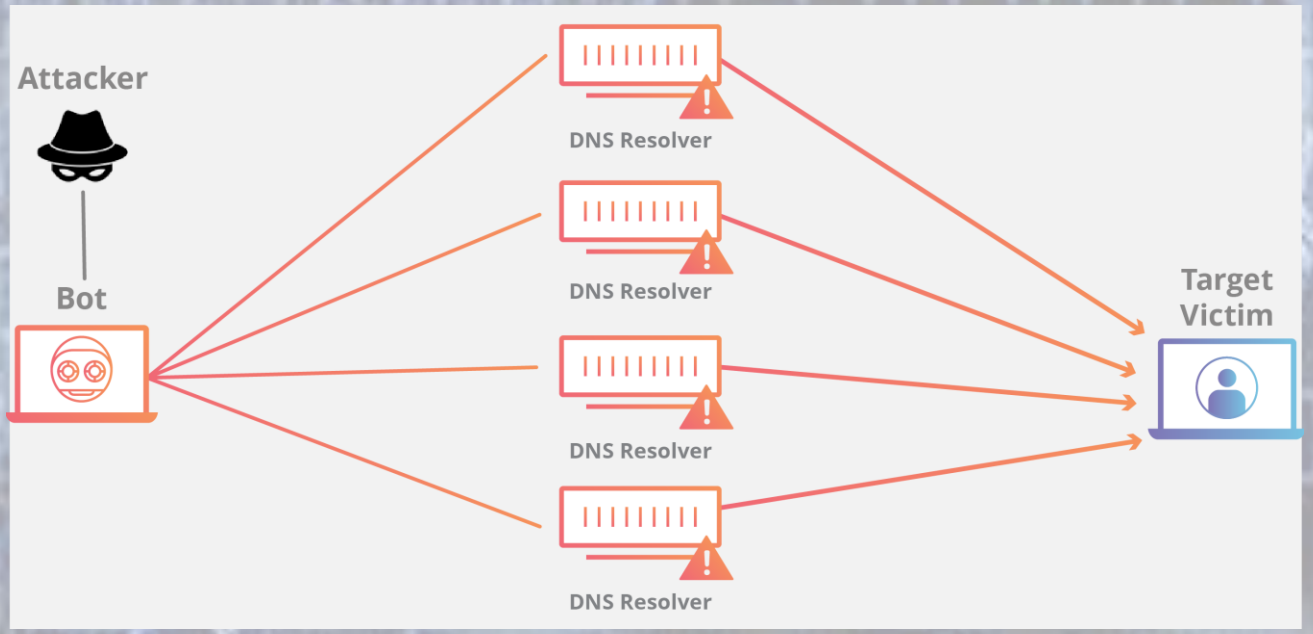
Inteligencia social

- **PHARMING -> Redirección a webs clonadas para robar datos**
- **MAN IN THE MIDDLE -> Sniffer de paquetes en la misma WiFi**

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

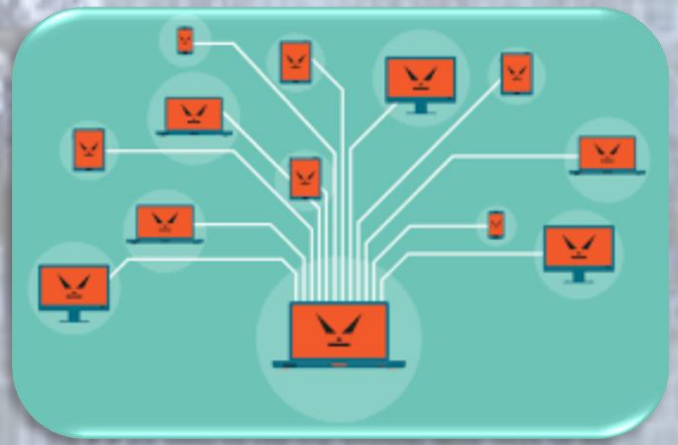
Otras clases de ataques

- **DDoS** (Denegación de servicio)
- **FUERZA BRUTA** (Diccionario)

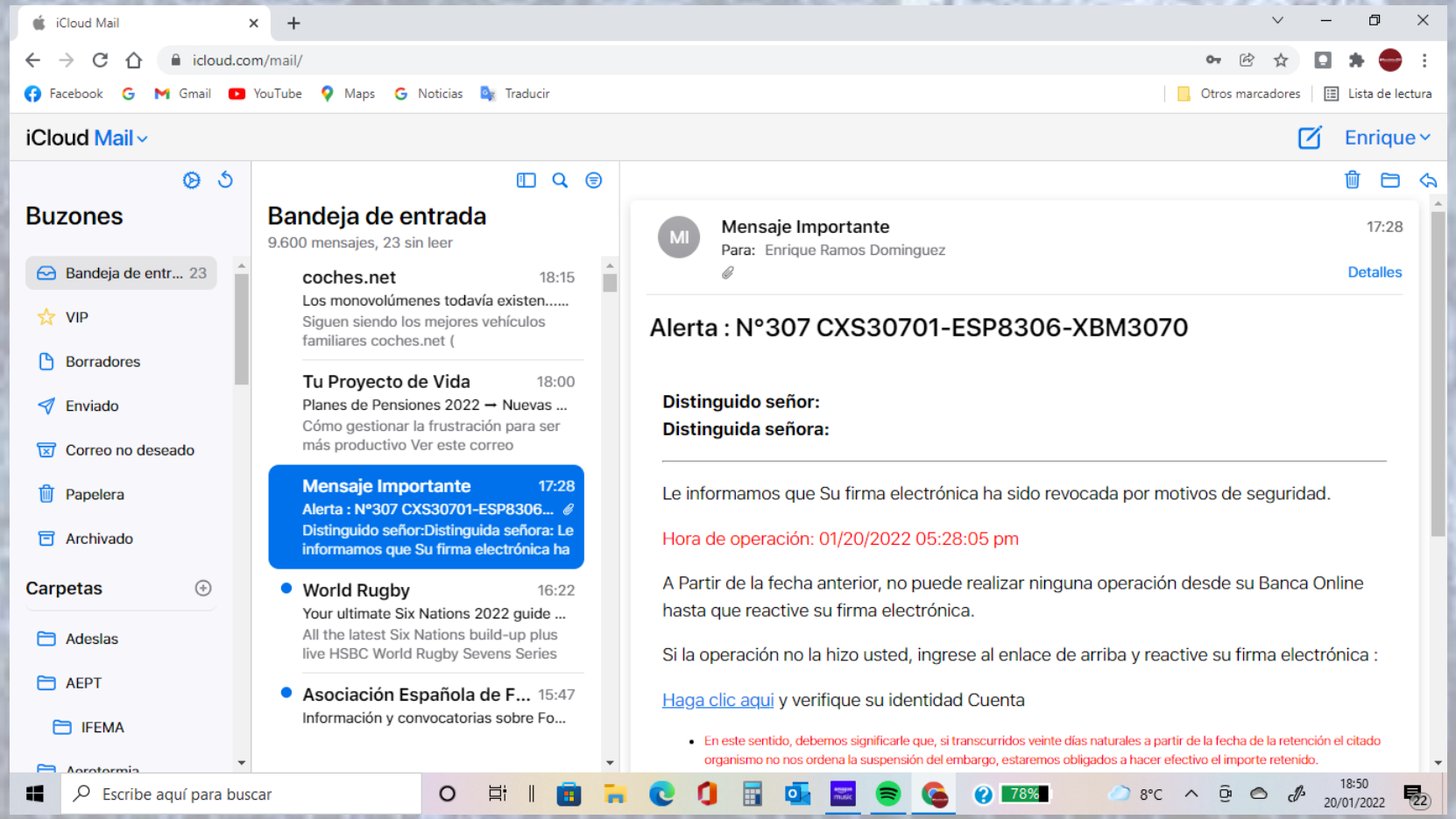


Otras clases de ataques

- **SQL INJECTION** -> Acceso a la BBDD de una web
- **BOTNET** (Ejército Zombie)



Caso Real



Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

índice de materias

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

Repercusiones de un ciberataque

Daños propios

Robos de identidad digital

- **Credenciales,**
- **Certificados electrónicos**
- **Datos biométricos**
- **Etc.**

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

Pérdidas de información

Repercusiones de un ciberataque

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

Repercusiones de un ciberataque

Fraude/ extorsión cibernética

- **Ingeniería social y malware (principalmente ransomware)**

Paralización de actividad

- **Desde unos días hasta meses.**

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

Repercusiones de un ciberataque

Gastos humanos

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

Repercusiones de un ciberataque

Sanciones administrativas

- **Plazo de 72 horas para notificar brecha a la AEPD. Sanciones desde 40.000 € y hasta 20 millones de euros o 4% de la facturación anual**

600.000€ de sanción por notificación tardía de una brecha de seguridad

Durante el presente mes de marzo, la Agencia Española de Protección de datos, ha emitido una resolución por la que acuerda sancionar a una aerolínea española de 600.000€ por la notificación tardía de una brecha de seguridad con más de 489.000 implicados, sin justificación válida para dicho retraso en la notificación.

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

Repercusiones de un ciberataque

Reclamaciones de terceros

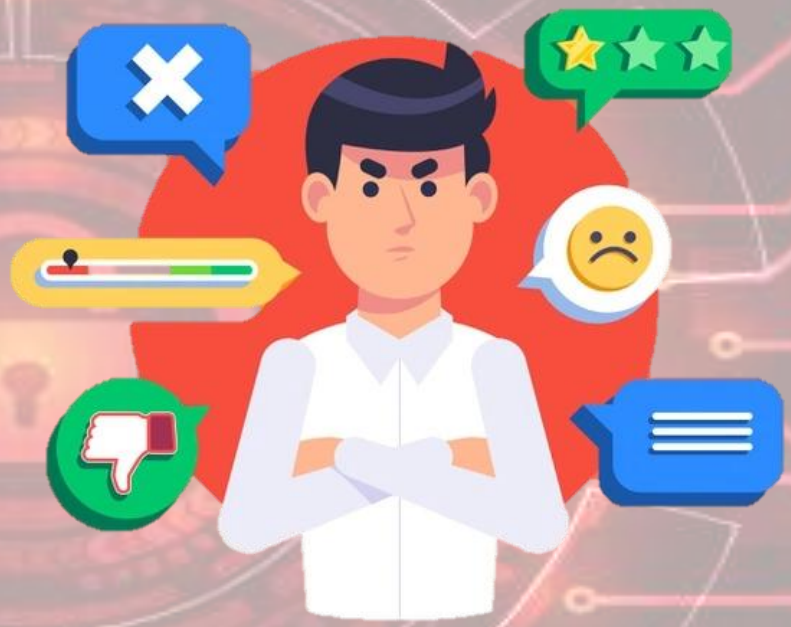
- Clientes, empleados y proveedores cuyos datos hayan sido expuestos
-

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

Repercusiones de un ciberataque

Daños reputacionales

- **Pérdida de confianza de clientes, proveedores e inversores**



Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

Repercusiones de un ciberataque

Cierre de negocio

6 de cada 10 PYMEs desaparece a los 6 meses de sufrir un ciberataque

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

índice de materias

- 05. Prevención de un ciberataque
  - Software original y actualizado
  - Webs Http
  - Contraseñas
  - Back up

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

¿Cómo prevenir un ciberataque?

1) SOFTWARE ORIGINAL

- El software pirata presenta mayor cantidad de vulnerabilidades
- A menudo los cracks (activadores) contienen malware

2) MANTENER SOFTWARE ACTUALIZADO

- Sistema operativo, programas, aplicaciones, complementos, etc.

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

¿Cómo prevenir un ciberataque?

3) EVITAR WEBS HTTP

4) CONTRASEÑAS SEGURAS Y 2FA

- El 2FA no es infalible, aunque supone una capa extra de seguridad.

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

¿Cómo prevenir un ciberataque?

5) Correo electrónico

- Desactivar descarga automática de archivos (desde aplicaciones)
- Descargar sólo archivos de confianza, y analizarlos antes de su apertura
- Evitar conectarse desde redes wifi públicas y/o sin seguridad WPA2. Preferible con datos móviles en tales casos
- Cifrar correos entrantes y salientes con protocolo TLS/SSL
- No hacer clic sobre enlaces de remitentes desconocidos o poco fiables
- Cerrar sesión al terminar (desde navegador)

¿Cómo prevenir un ciberataque?

6) Análisis de vulnerabilidades (pentesting)

Pentesting

Conoce tus debilidades para corregirlas

7) Antivirus

- Actualizado, correctamente configurado y realizar análisis periódicamente. Aplicable a sistemas operativos de escritorio y móviles

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

¿Cómo prevenir un ciberataque?

8) BACKUP: Regla 3-2-1

9) ALMACENAMIENTO EXTERNO:

- **Deshabilitar la apertura automática**
- **Analizar antes de abrir**
- **Cifrar contenido sensible**

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

¿Cómo prevenir un ciberataque?

10) REFORZAR SEGURIDAD ROUTER:

- Actualizar firmware
- Cambiar SSID y contraseña WiFi de fábrica
- Cambiar contraseña WiFi con asiduidad
- Cambiar credenciales predeterminados de acceso al router
- Establecer protocolo de seguridad WPA2-AES
- Configurar firewall

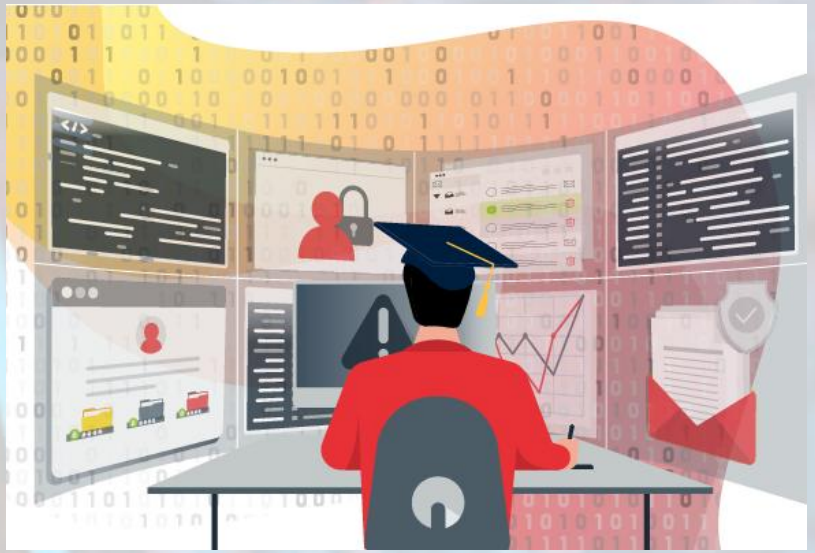
Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

¿Cómo prevenir un ciberataque?

11) DESCARGAR SOFTWARE SÓLO DESDE FUENTES DE CONFIANZA

- **Verificados por la propia Store del sistema operativo, o suministrado a través del propio fabricante/desarrollador**

12) Formación



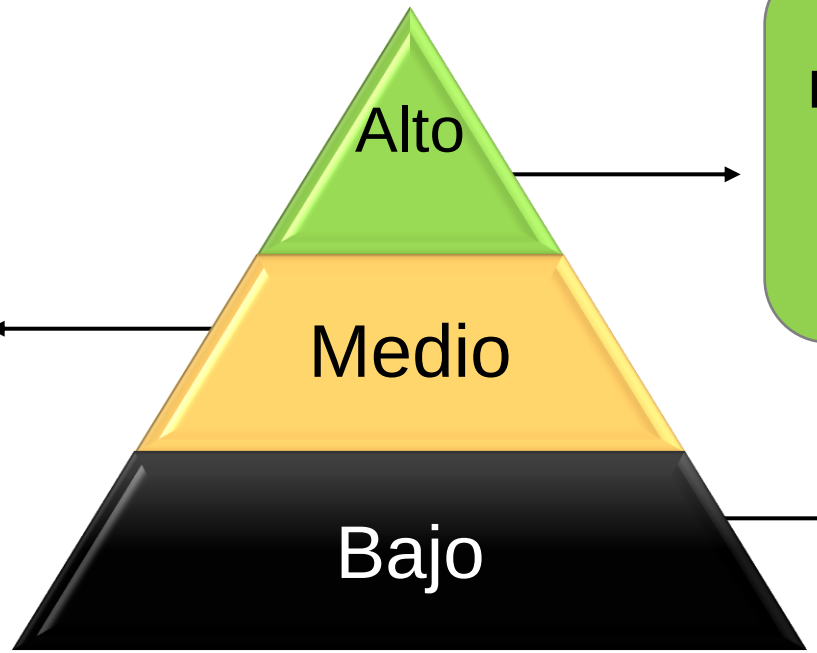
Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

índice de materias

- 06. Gestión del incidente
  - Fases
  - Ciberseguro

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

Grado de madurez cibernética en una empresa



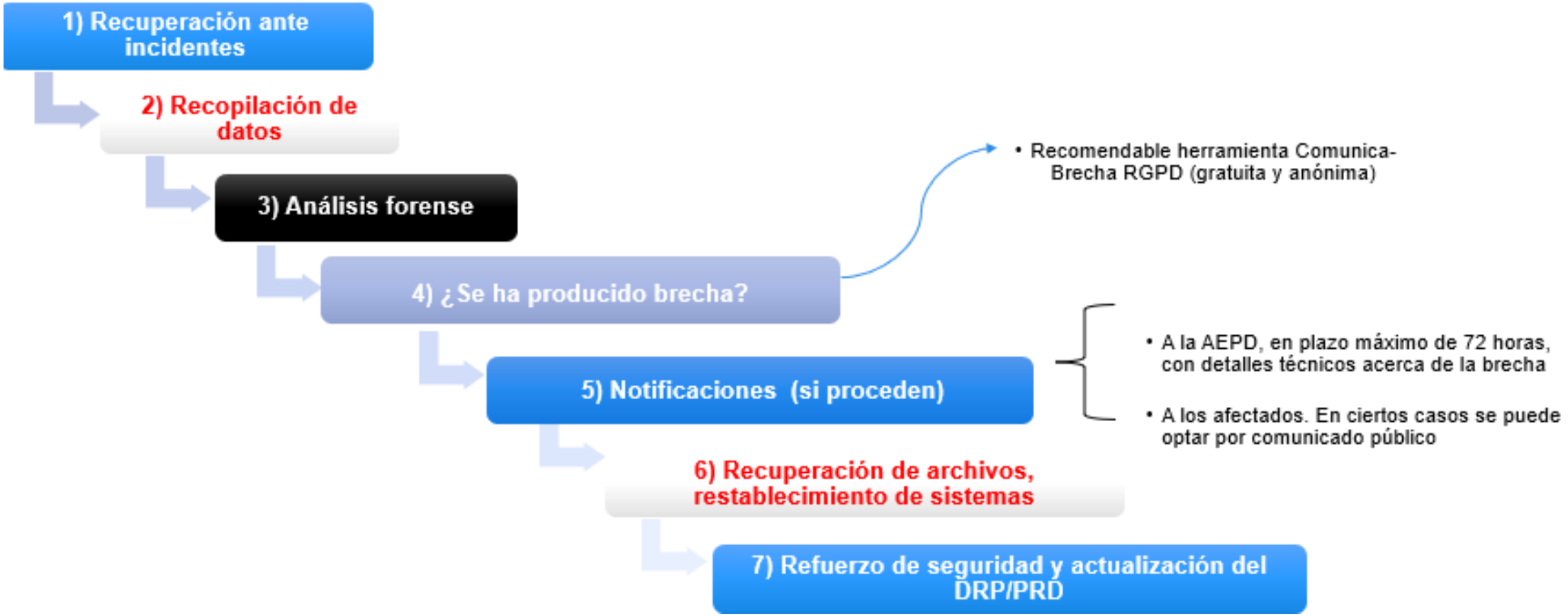
Incorpora Plan de Recuperación ante Desastres (actualizable) y continuidad de negocio. También incorpora ciberseguro

Combina con formación continua, pentesting frecuente y medidas de monitorización y detección de intrusiones

Sólo tecnología para prevención

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

FASES DE LA GESTIÓN TÉCNICA DE INCIDENTES



COBERTURAS de CIBERSEGURO

Gestión técnica de incidentes

-Gastos de defensa y fianzas

-Gastos de emergencia

-Daños propios

Fraude y extorsión cibernéticos

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

COBERTURAS de CIBERSEGURO

-Sanciones administrativas

-Responsabilidad ante terceros

-Pérdidas de beneficios

-Restitución de imagen

-Etc.

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

Datos de la AEPD 2022

Reclamaciones planteadas con mayor frecuencia	2020	2021	% relativo	Δ% anual
TOP 10	**7.727**	**10.840**	**78%**	**40%**
Servicios de Internet	1.602	2.220	16%	39%
Videovigilancia	1.189	1.736	12%	46%
Publicidad (excepto spam)	681	1.528	11%	124%
Ficheros de morosidad	1.510	1.284	9%	-15%
Reclamación de deudas	656	859	6%	31%
Administración pública	503	740	5%	47%
Sanidad	388	680	5%	75%
Comercios, transporte y hostelería	405	663	5%	64%
Entidades financieras/acreedoras	437	643	5%	47%
Publicidad a través de e-mail o teléfono móvil	356	487	4%	37%
Otros	**2.597**	**3.065**	**22%**	**18%**
TOTAL	**10.324**	**13.905**	**100%**	**35%**

MUCHAS GRACIAS POR SU ATENCION

Recoletos ERD
Consultores de Seguros & Gestión de Riesgos

CONTACTO:
Enrique Ramos
Teléfono 664 670 785
Mail:
eramos@recoletosconsultores.es