DIPUTACIÓN DE BURGOS

LA SEGURIDAD DE LA INFORMACIÓN EN TU AYUNTAMIENTO

"Estamos libres de amenazas"

SIN CLASIFICAR

El cambio es exponencial

Sociedad agraria

4000 a.C. ~ 1763

Consumo medio de proteínas per cápita

Sociedad industrial

1764 ~1970

Consumo medio de electricidad per cápita

Sociedad de Internet

1971 ~ 2014

Penetración de internet

Sociedad de los datos

Después de 2015

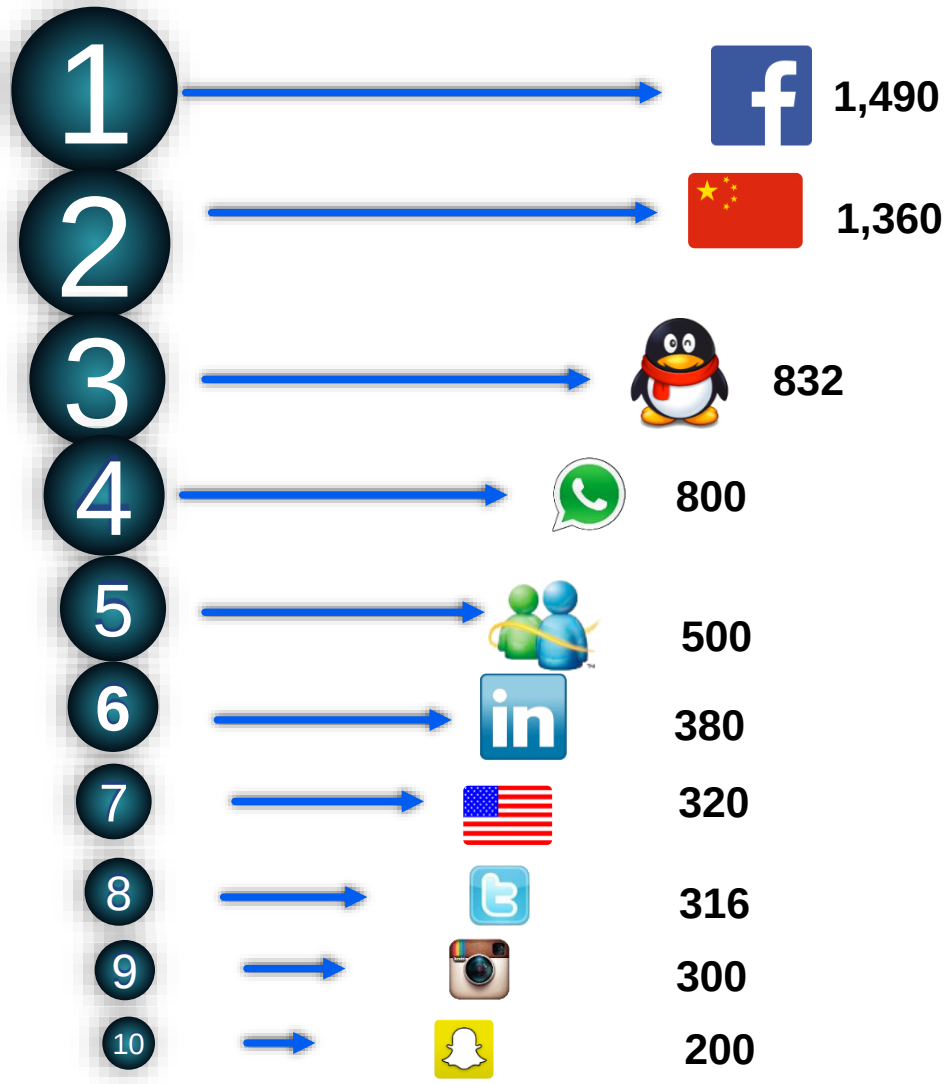
Consumo medio de información per cápita

OCT 2015

Las **REDES SOCIALES** tienen un

IMPACTO

instantáneo y masivo



La disrupción en servicios es cada vez más rápida

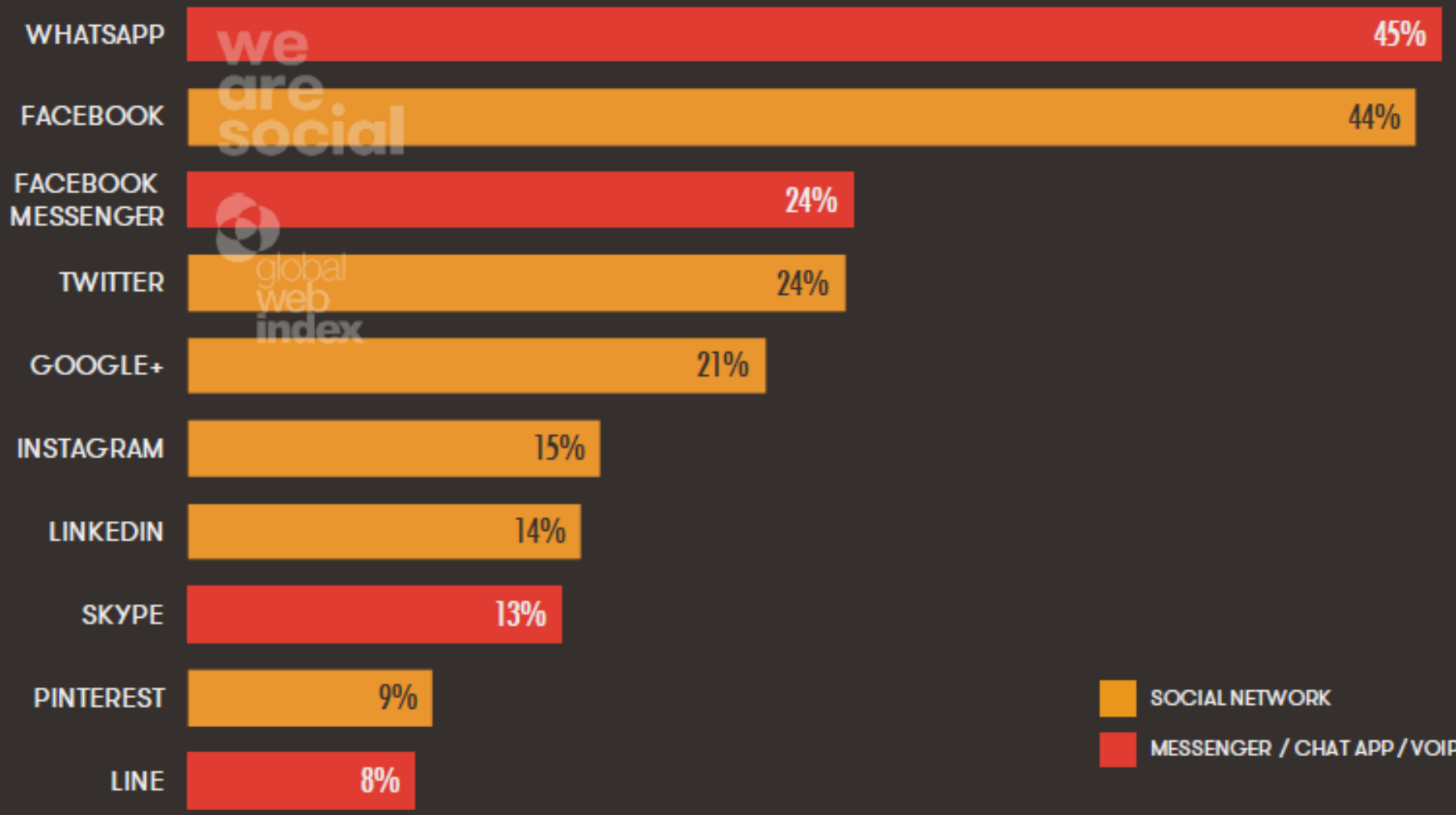
Tiempo necesario para alcanzar 100 millones de usuarios

Si no estás pagando por el producto,

JAN 2016

TOP ACTIVE SOCIAL PLATFORMS

SURVEY-BASED DATA: FIGURES REPRESENT USERS' OWN CLAIMED / REPORTED ACTIVITY



ÍNDICE

1. CCN / CCN-CERT

2. INFORME ANUAL DE LA AMENAZA

3. CONCIENCIACIÓN

El CCN actúa según el siguiente marco legal:

Ley 11/2002, 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), que incluye al Centro Criptológico Nacional (CCN)

Real Decreto 421/2004, 12 de marzo, que regula y define el ámbito y funciones del CCN.

Orden Ministerio Presidencia PRE/2740/2007, de 19 de septiembre, que regula **el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información**

Real Decreto 3/2010, de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica**
RD 951/2015, 4 de Noviembre. Actualización

MARCO LEGAL

Real Decreto 3/2010, 8 de Enero, que define el **Esquema Nacional de Seguridad** para la Administración Electrónica. **RD 951/2015, 4 de Noviembre. Actualización**

Establece al CCN-CERT como Centro de Respuesta a Ciberincidentes Gubernamental/Nacional

MISIÓN

Contribuir a la mejora de la **ciberseguridad española**, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a las **Administraciones Públicas** y a las **empresas** consideradas de interés **estratégico**, y afrontar de forma activa las nuevas ciberamenazas.

- **Sistemas de información clasificados**
- **sistemas de la Administración**
- **Sistemas** de empresas de interés **estratégicos.**

Actividades del CCN

Desarrollo

Art 2. Apdo.2e RD 421/2004: Coordinar la promoción, desarrollo, obtención, adquisición, explotación y uso de tecnologías de seguridad

- Conocimiento amenazas
- Necesidades operativas
- Estado tecnología seguridad
- Conocimiento industria sector

Evaluación

Art 2. Apdo.2d RD 421/2004: Valorar y acreditar capacidades de productos de cifra para manejar información de forma segura

- Seguridad funcional
- Criptológica
- TEMPEST

Certificación

Art 2. Apdo.2c RD 421/2004: Constituir el organismo de certificación del Esquema Nacional de Evaluación y Certificación del ámbito STIC

- Seguridad funcional
- Criptológica
- TEMPEST

Productos para Seguridad TIC

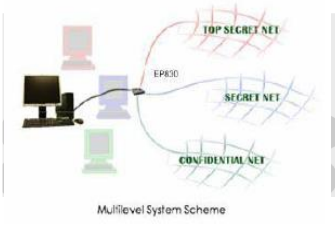
Borrado Seguro Datos

TEMD

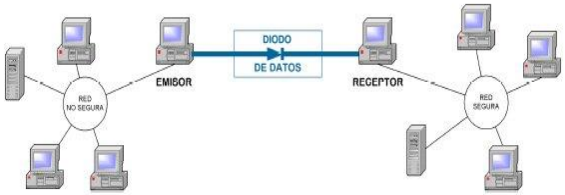
Ordenador Seguro

Herramienta PILAR

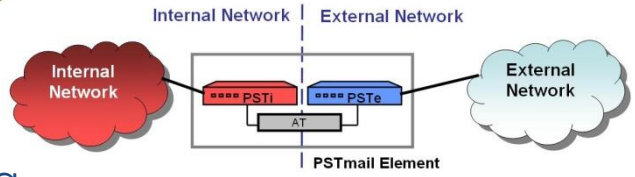
Sistema Multidominio



Diodo Datos



Pasarela Segura Correo y Ficheros



Productos de Cifra Nacionales

- Cifrador IP alta velocidad EP430GN
- Cifrador IP táctico EP430T
- Cifrador SCIP Satélite (CRIPTOPER SAT)
- Terminales Móviles Seguros
- Terminal de voz y video SCIP (EP641)

Actividades del CCN

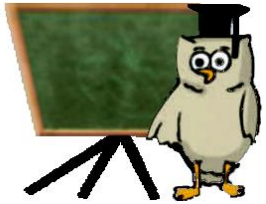
Normativa

Art 2. Apdo.2a RD 421/2004: Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de las TIC

- Desarrollo normas, procedimientos, instrucciones y guías: Serie CCN-STIC
- + de 262 guías

Formación

Art 2. Apdo.2b RD 421/2004: Formar al personal de la Administración especialista en el campo de la seguridad de las TIC



- Concienciación
- Cursos STIC

Velar

Art 2. Apdo.2f RD 421/2004: Velar por el cumplimiento normativa relativa a la protección de la información clasificada en Sistemas TIC

- Inspecciones técnicas STIC
- Análisis vulnerabilidades
- Auditorías de seguridad

Actividades del CCN

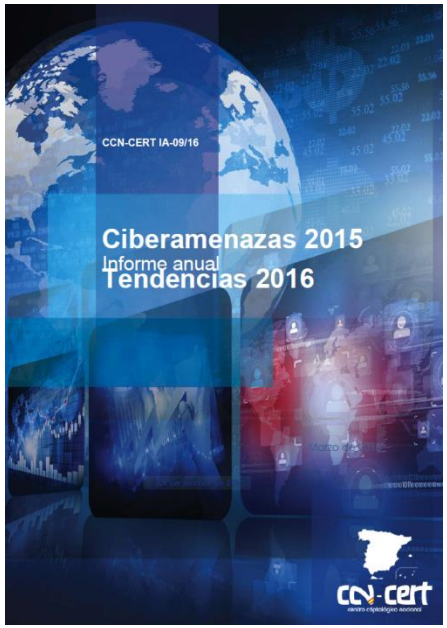
Detección de la Amenaza

Ley 11/2007 y Real Decreto 3/2010, 8 de Enero, que define el Esquema Nacional de Seguridad para la Administración Electrónica. RD 951/2015, 23 de octubre. Actualización

Gestión de Incidentes

Real Decreto 3/2010, 8 de Enero, que define el Esquema Nacional de Seguridad para la Administración Electrónica. RD 951/2015, 23 de octubre. Actualización

- Diversidad de fuentes de información
- Sistemas de Alerta
- Ingeniería Inversa
- Análisis forense
- Sistemas de gestión de incidentes
- Sistemas de intercambio de información



INFORME ANUAL DE AMENAZAS 2015
TENDENCIAS 2016

Definiciones. Agentes de la amenaza

CIBERSEGURIDAD

La habilidad de proteger y defender las redes o sistemas de los **ciberataques.** Estos según su motivación pueden ser:

CIBERESPIONAJE

Ciberataques realizados para obtener secretos de estado, propiedad industrial, propiedad intelectual, información comercial sensible o datos de carácter personal.

CIBERDELITO / CIBERCRIMEN

Actividad que emplea las redes y sistemas como medio, objetivo o lugar del delito.

CIBERACTIVISMO o HACKTIVISMO

Activismo digital antisocial. Sus practicantes persiguen el control de redes o sistemas (sitios web) para promover su causa o defender su posicionamiento político o social.

CIBERTERRORISMO

Actividades dirigidas a causar pánico o catástrofes realizadas en las redes y sistemas o utilizando éstas como medio.

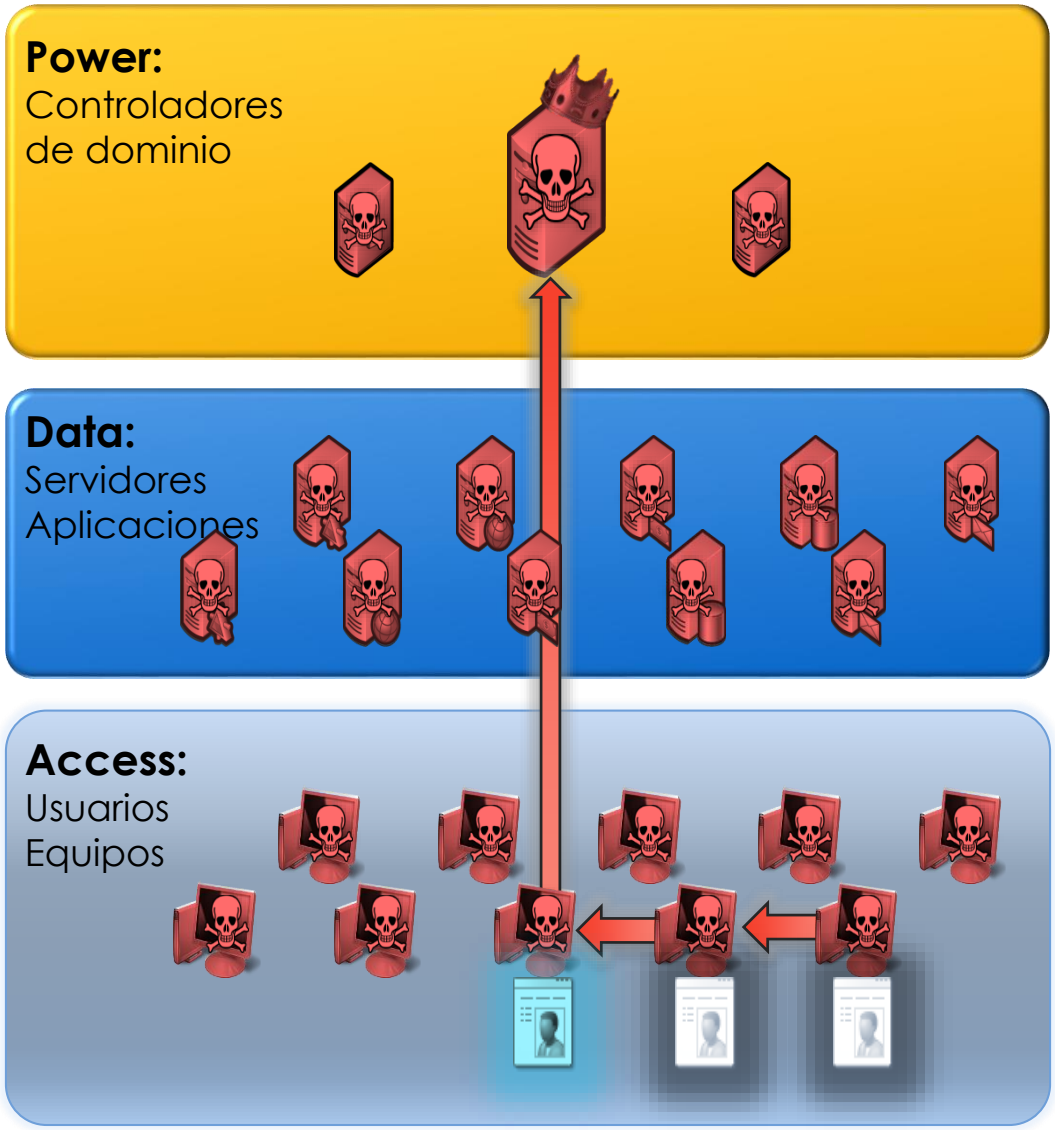
CIBERCONFLICTO / CIBERGUERRA

CIBERATAQUE

Uso de redes y comunicaciones para acceder a información y servicios sin autorización con el ánimo de robar, abusar o destruir.

Año	Concepto Seguridad	Amenaza	Cambios Tecnológicos
1980-90	Compusec Netsec Transec	Naturales	Telecomunicaciones Sistemas Clasificados
1990-2004	Infosec Info. Assurance	Intencionadas	Redes corporativas Sist. Control industrial Infraestructuras Criticas
2005-2010	Ciberseguridad Ciberdefensa	Ciberespionaje Ciberterrorismo	Telefonía móvil Redes sociales Servicios en Cloud
2010-2015	Ciberresiliencia Seg. Transparente Defensa activa	Ciberguerra APT Hacktivismo Ciberactivismo	BYOD Shadow IT …//…

Tomando el control



1. Objetivos en masa / definidos
2. Usuarios con altos privilegios son el principal objetivo
3. Buscan credenciales "de lo que sea"
4. Búsqueda de credenciales cacheadas, cuentas de acceso a dominio, correo electrónico, etc..
5. Si logran acceder a toda la red, la empresa está perdida

Ciberamenazas. Agentes. Conclusiones 2015

1. Ciberespionaje / Robo patrimonio tecnológico, propiedad intelectual
   - China, Rusia, Irán, otros…
     - Servicios de Inteligencia / Fuerzas Armadas / Otras empresas

2. Ciberdelito / cibercrimen
   - HACKERS y crimen organizado

Usuarios internos

3. Ciberactivismo
   - ANONYMOUS y otros grupos

4. Uso de INTERNET por terroristas
   - Objetivo : Comunicaciones , obtención de información, propaganda, **radicalización** o financiación

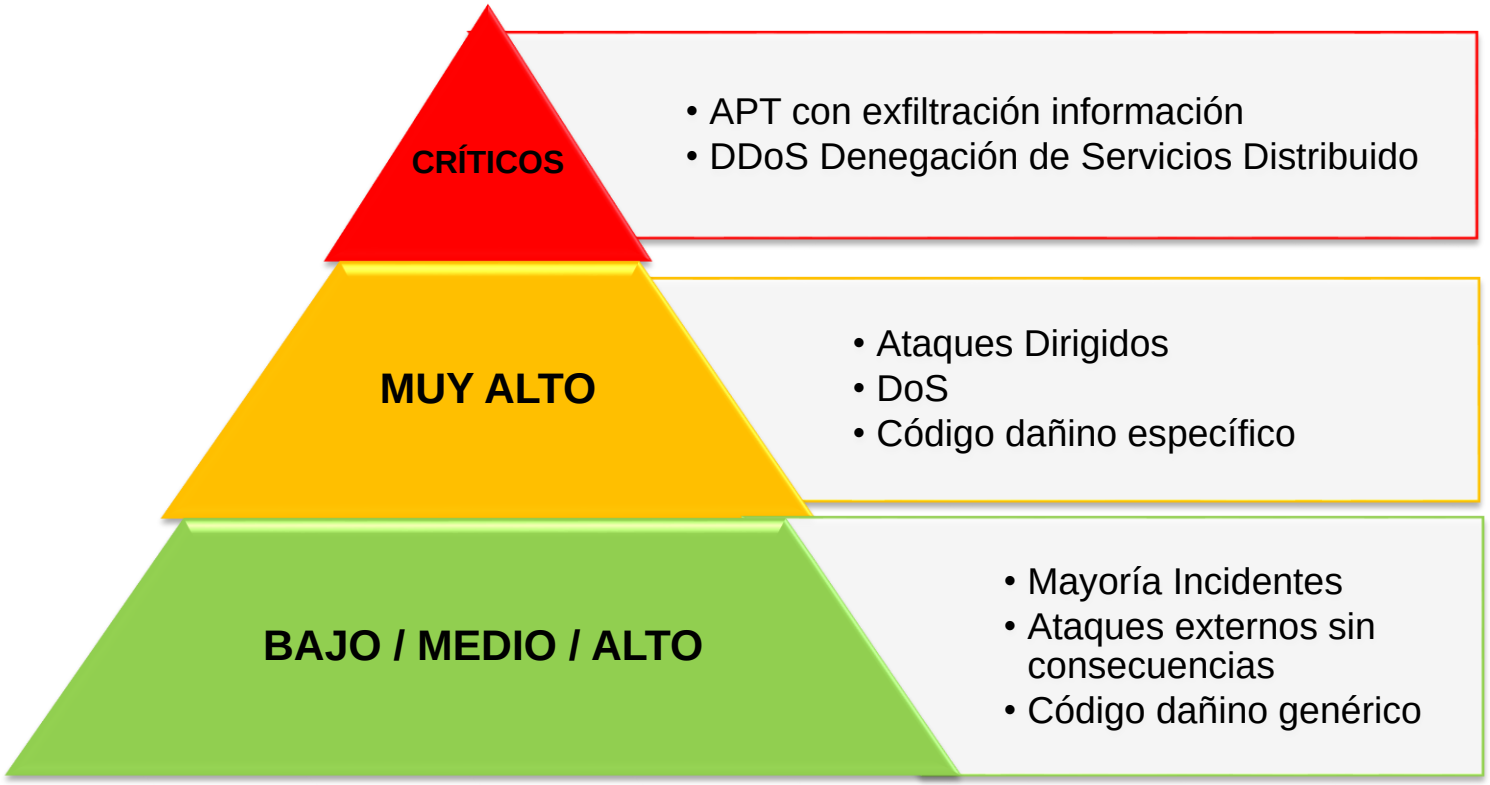
5. Ciberterrorismo
   - Ataque a Infraestructuras críticas y otros servicios

¿CIBERYIHADISMO?

AGENTES DE LA AMENAZA TENDENCIAS

- **Ciberespionaje** continuará en **ascenso** al tiempo que lo hace en **sofisticación y peligrosidad**.
- **Ciberdelito** los **beneficios** obtenidos propiciará el **incremento de estas acciones**
- **Ciberterrorismo** gran peligrosidad **potencial**
- **Ciberyihadismo** no ha hecho sino empezar a mostrarse es de esperar **más ataques**
- Resto amenazas y actores internos no se prevén alteraciones sustanciales de comportamiento

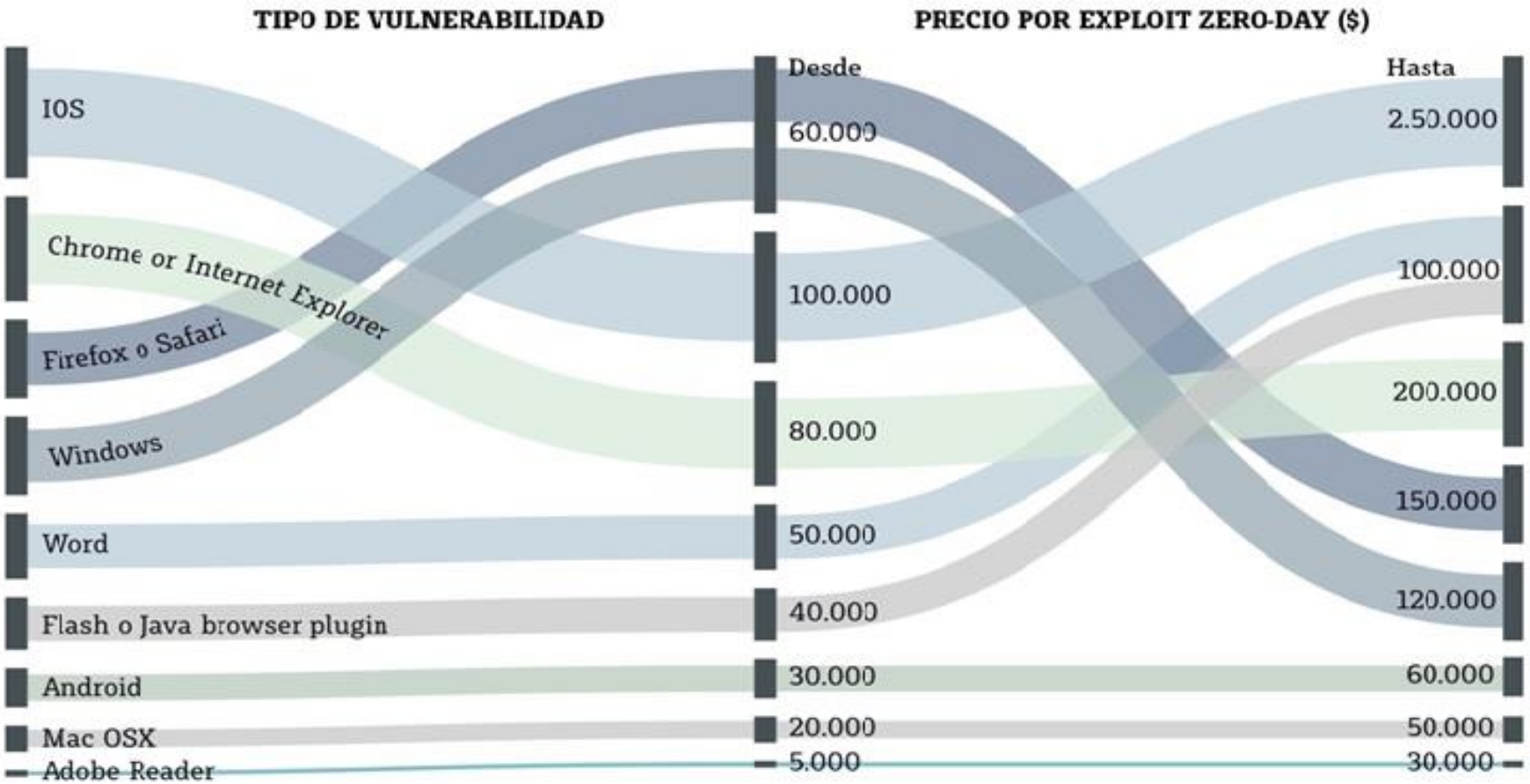
Gestión de Ciberincidentes (CCN-STIC-817)



HERRAMIENTAS UTILIZADAS POR LOS ATACANTES

- En comparación con 2014 el **nivel de amenazas se ha agravado considerablemente**
- Los **ciberatacantes están invirtiendo** en el desarrollo de **nuevos exploits-kits** y en la **búsqueda de nuevas vulnerabilidades**

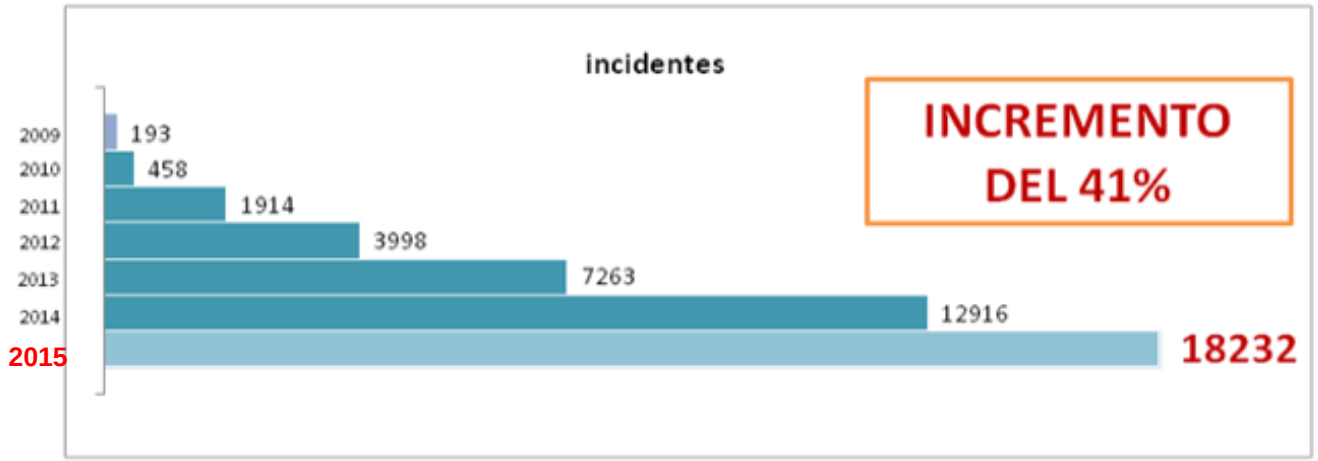
HERRAMIENTAS UTILIZADAS exploits día cero

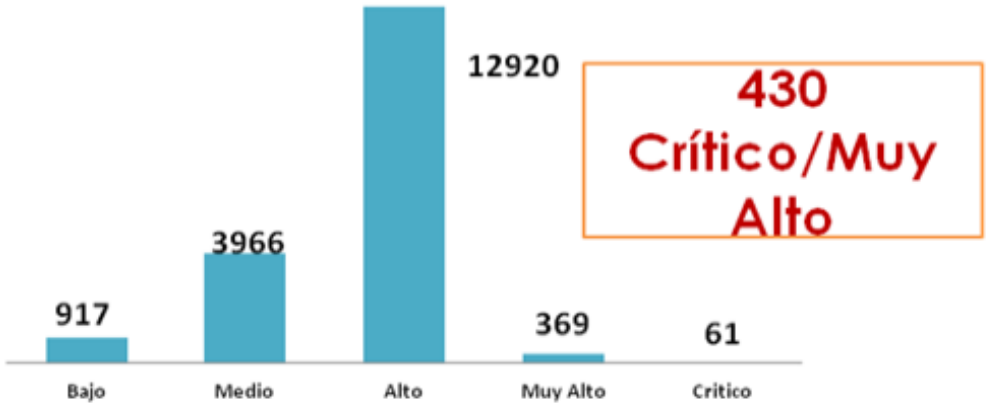


McAfee Labs Threats Report (Aug. 2015)

Incidentes detectados por los sistemas de alerta temprana del CCN-CERT

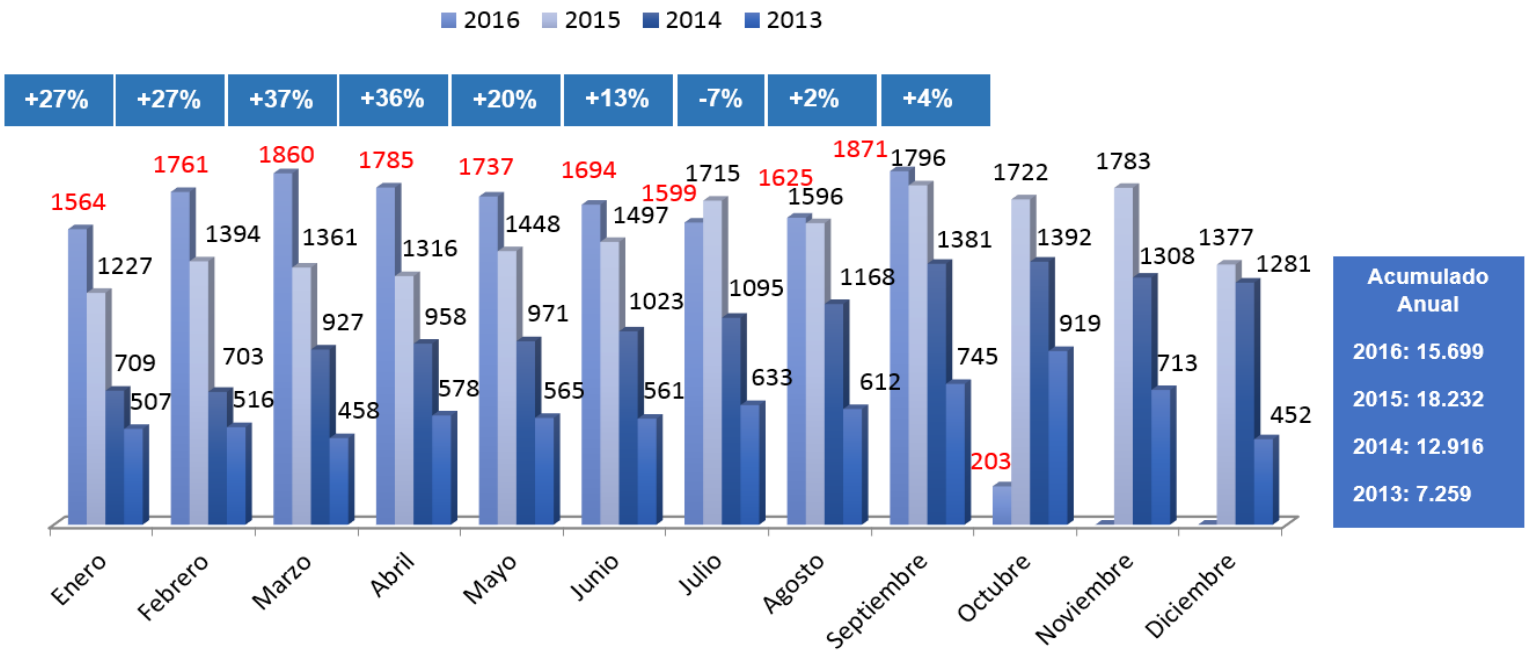
Total de incidentes gestionados por año

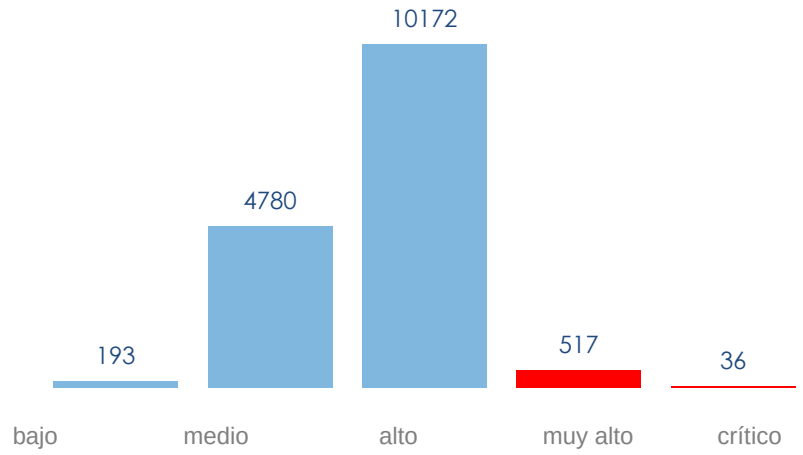




SIN CLASIFICAR

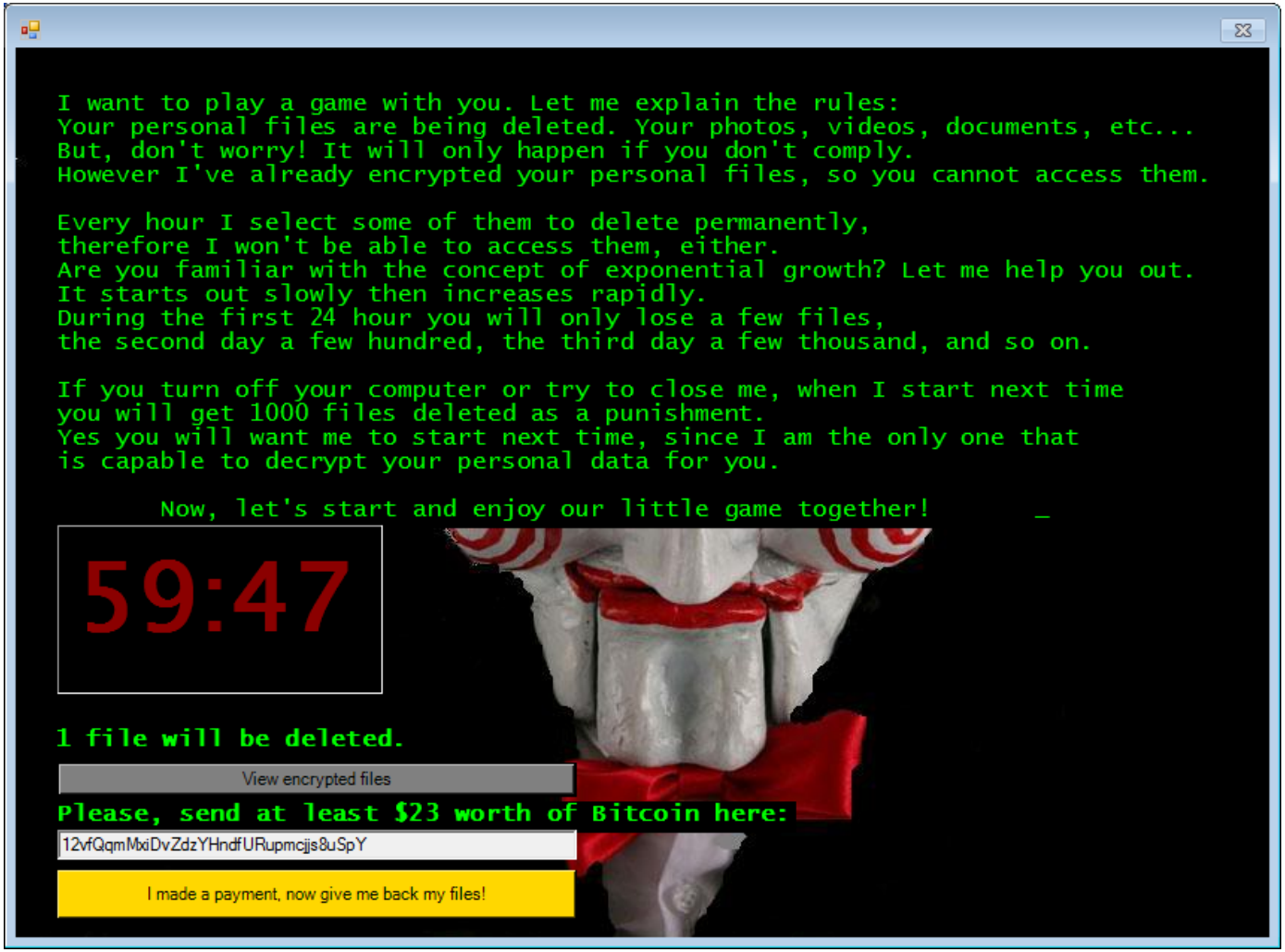
14.10.2016
16.156 INC.





553 críticos
y muy altos

75 % SAT INTERNET
15 % SAT SARA
10 % OTROS



Ransomware is helping make the cyber threat real.

Familia/Versión Ransomware: https://id-ransomware.malwarehunterteam.com/

Herramientas descifrado: https://www.nomoreransom.org/decryption-tools.html

2015

Tipo	Nº incidentes
Cryptolocker	93
Torrentlocker	89
Teslacrypt	73
Cryptowall	109
Otros	73

Total: 427

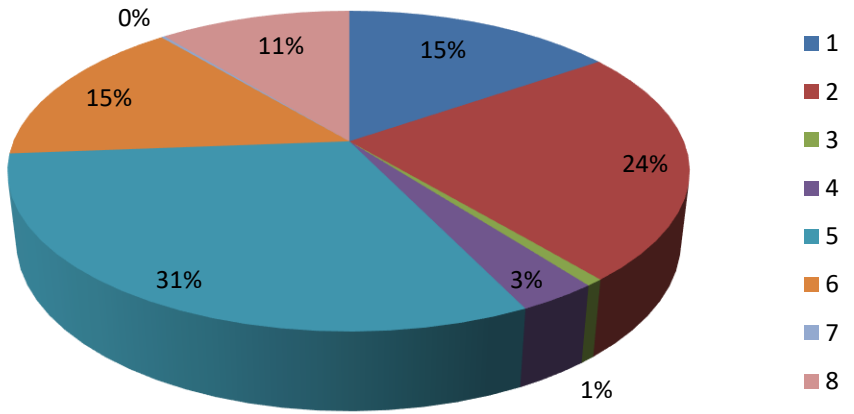
2016

Tipo	Nº incidentes
Locky	308
Teslacrypt	234
Torrentlocker	151
Cryptolocker	108
Cryptowall	153

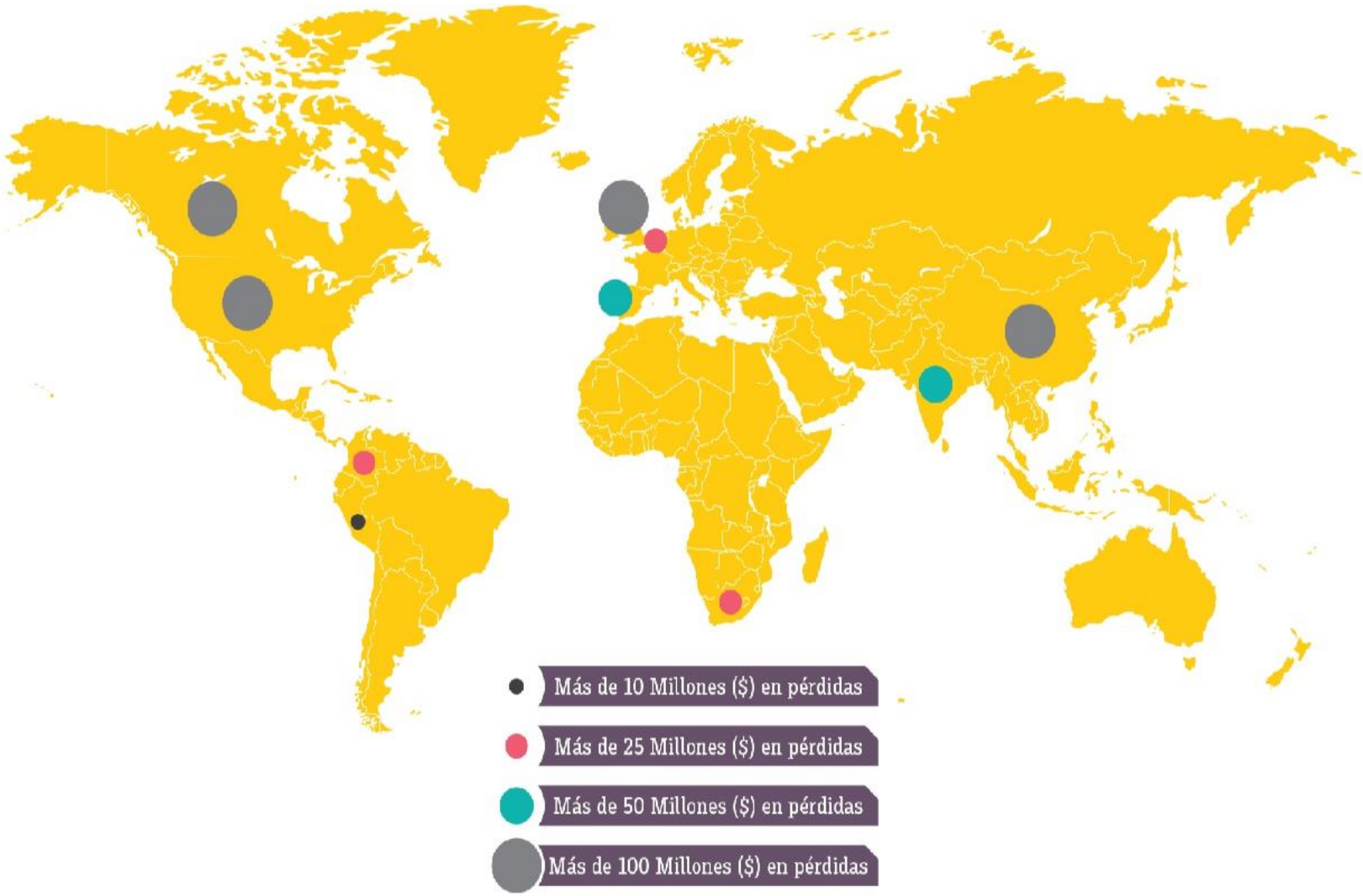
Total: 954

RAMSONWARE

PAGO DE RESCATE TRAS EL SECUESTRO DEL SISTEMA INFORMATICO”

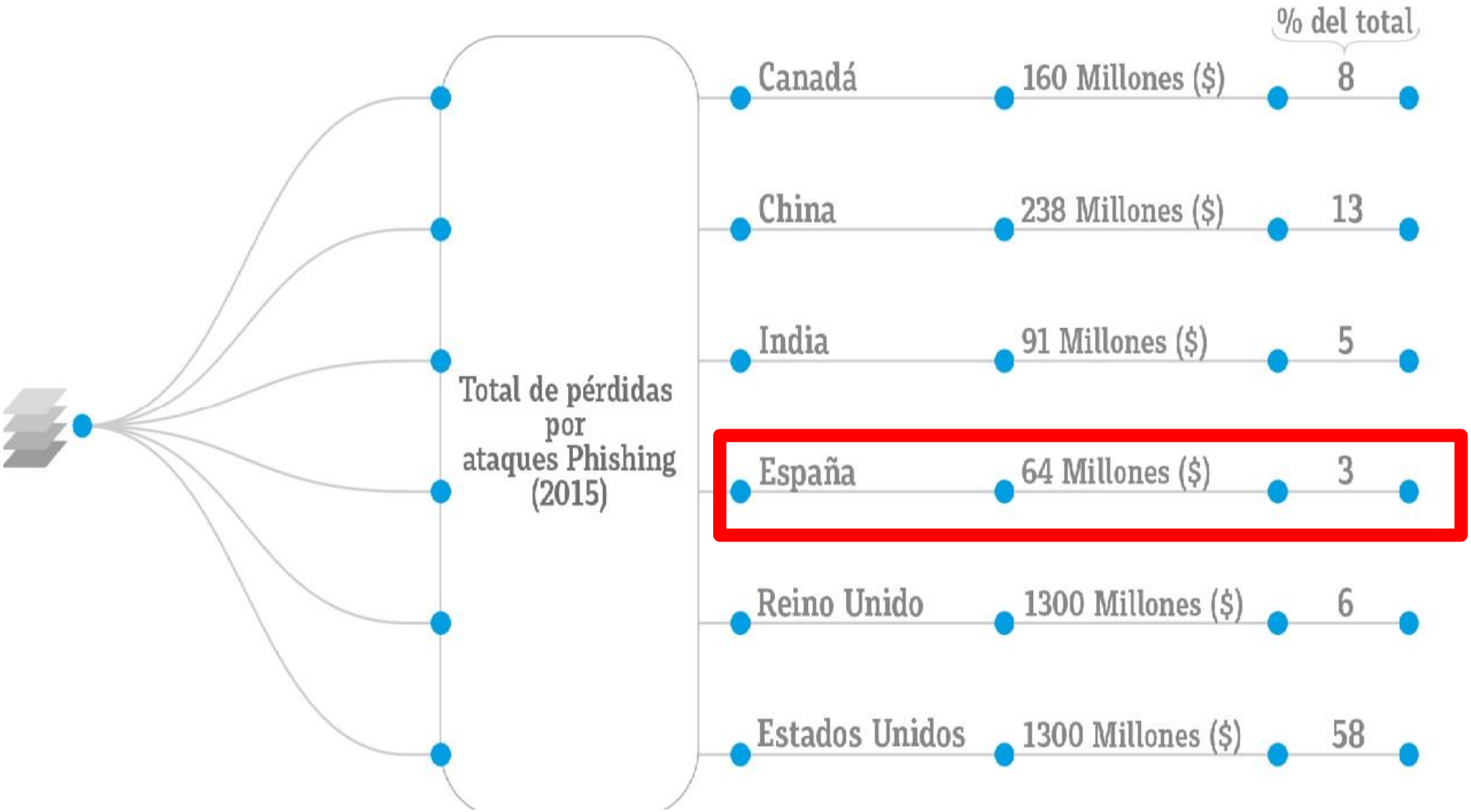


HERRAMIENTAS UTILIZADAS phishing paises con mayores perdidas



EMC-RSA http://spain.emc/microsites/rsa/phishing/index.htm

HERRAMIENTAS UTILIZADAS phishing paises con mayores perdidas



EMC-RSA http://spain.emc/microsites/rsa/phishing/index.htm

¿Qué hemos aprendido todos este tiempo sobre las **APT**?

Advanced Persistent Threat

- Ataque Dirigido

  Ciber Ataque "a medida" contra un objetivo concreto (administración, empresa, red, sistema).

- Threat

  El atacante tiene la intención y capacidades para ganar el acceso a información sensible almacenada electrónicamente.

- Persistent

  Una vez infectado, se mantiene el acceso a la red/sistema durante un largo periodo de tiempo

  Muy difícil de eliminar

- Advanced

  Habilidad de evitar la detección

  Se adapta al objetivo

  Disponibilidad de recursos tecnológicos, económicos, humanos


Saben más…


Son más…


Son muy insistentes…

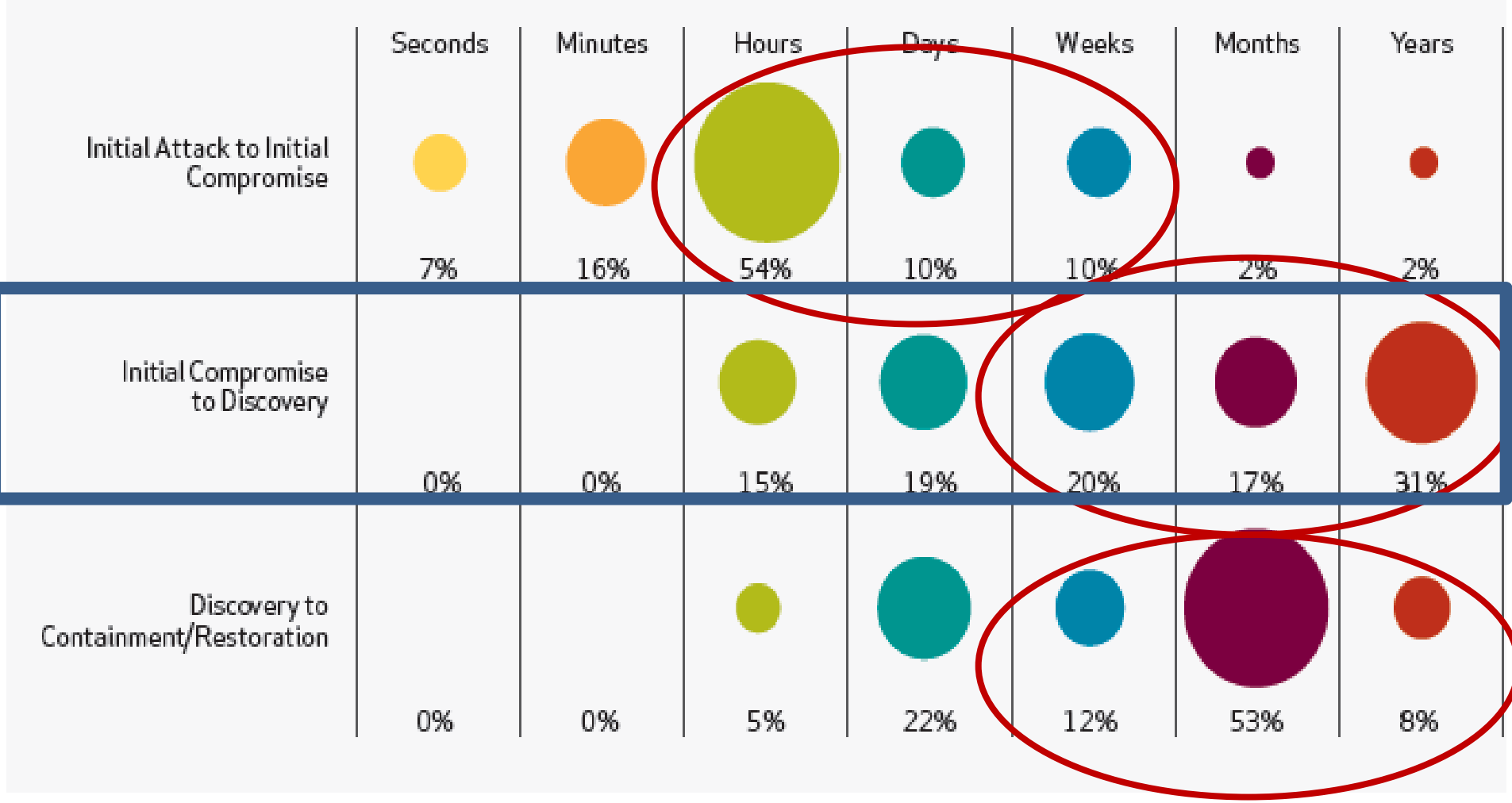

Están especializados…

Debilidades de Nuestros Sistemas de Protección

- ✓ **Falta de concienciación** y **desconocimiento del riesgo**
- ✓ **Somos objetivos blandos**: Sistemas con Vulnerabilidades, escasas configuraciones de seguridad y Seguridad Reactiva.
- ✓ **Poco personal de seguridad y escasa vigilancia**
- ✓ **Ausencia herramientas faciliten investigación**
- ✓ **Mayor superficie de exposición (Redes sociales, Telefonía móvil (BYOD) y Servicios en nube)**
- ✓ **Afectados NO comparten información.**
- ✓ **NO comunican incidentes**

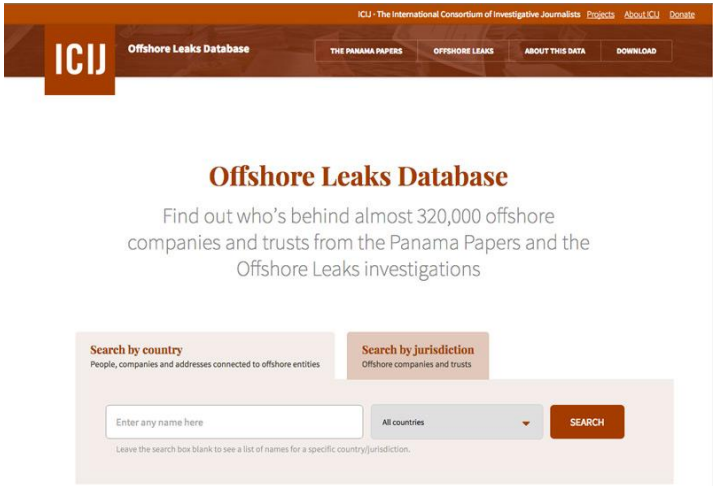
¿Me puede **pasar a mí**?

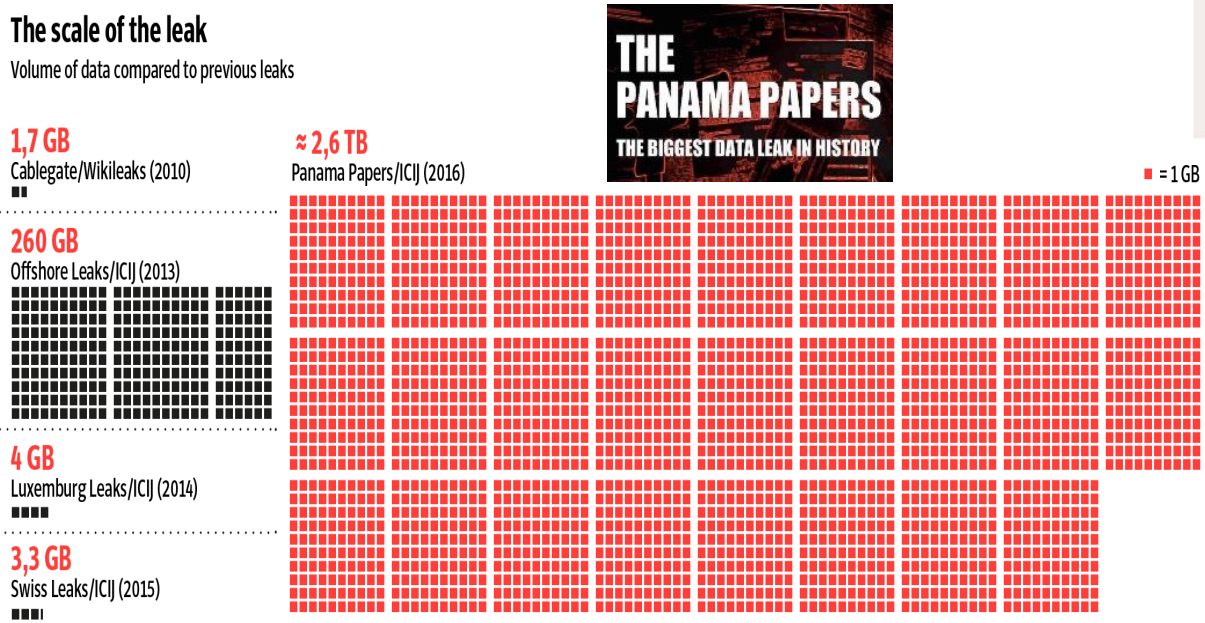
¿ Impacto en las organizaciones?

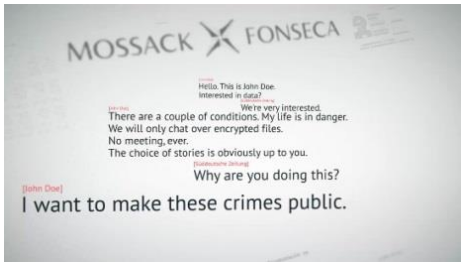


VERIZON rp_data-breach-investigations 2012

Los beneficios obtenidos y el acceso cada vez más fácil a las herramientas de ataque propicia el incremento del número de ciberdelincuentes y, en consecuencia, el de sus acciones.







Esquema Nacional de Seguridad

ens Esquema Nacional de Seguridad

de aplicación a todas las AA.PP.

BOLETÍN OFICIAL DEL ESTADO

Núm. 25 Viernes 29 de enero de 2010 Sec. I. Pág. 8089

I. DISPOSICIONES GENERALES

MINISTERIO DE LA PRESIDENCIA

1330 *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.*

RD 3/2010 (08.01.2010)

BOLETÍN OFICIAL DEL ESTADO

Núm. 264 Miércoles 4 de noviembre de 2015 Sec. I. Pág. 104246

I. DISPOSICIONES GENERALES

MINISTERIO DE LA PRESIDENCIA

11881 *Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.*

RD 951/2015 (23.10.2015)

ens Esquema Nacional de Seguridad

1. Los **Principios básicos,** que sirven de guía.
2. Los **Requisitos mínimos,** de obligado cumplimiento.
3. La **Categorización de los sistemas** para la adopción de **medidas de seguridad** proporcionadas.
4. La **auditoría de la seguridad** que verifique el cumplimiento del ENS.
5. La **respuesta a incidentes de seguridad**. Papel del CCN- CERT.
6. El uso de **productos certificados**. Papel del Organismo de Certificación (CCN).
7. La **formación y concienciación**.

¿Qué puedo hacer **yo**?

Vector de entrada - Ingeniería Social

- En el 75% de los casos se utilizan ataques de *spear phishing* para conseguir la infección de la red objetivo.

- ¿En qué consiste el *spear phishing*?
  - Correo electrónico **especialmente diseñado** para engañar al receptor y obtener datos sensibles de éste.

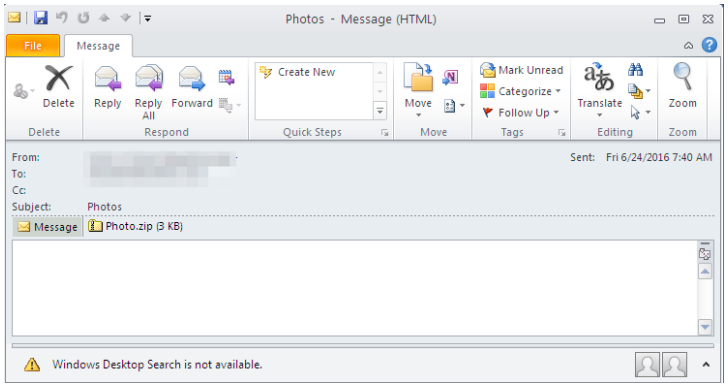
- ¿En qué se diferencia del *phishing*?
  - El *phishing* está pensado para engañar a un **elevado número de víctimas**, mientras que el *spear phishing* se centra únicamente en **objetivos concretos**.

Vector de infección. Correo electrónico

- En el 75 % de los casos se utiliza **Spear Phishing (pesca dirigida)** para conseguir la infección del objetivo.
  - Correo electrónico **especialmente diseñado** para engañar al receptor y obtener datos sensibles del mismo.
  - Se centra en **objetivos concretos.**

Analizar:

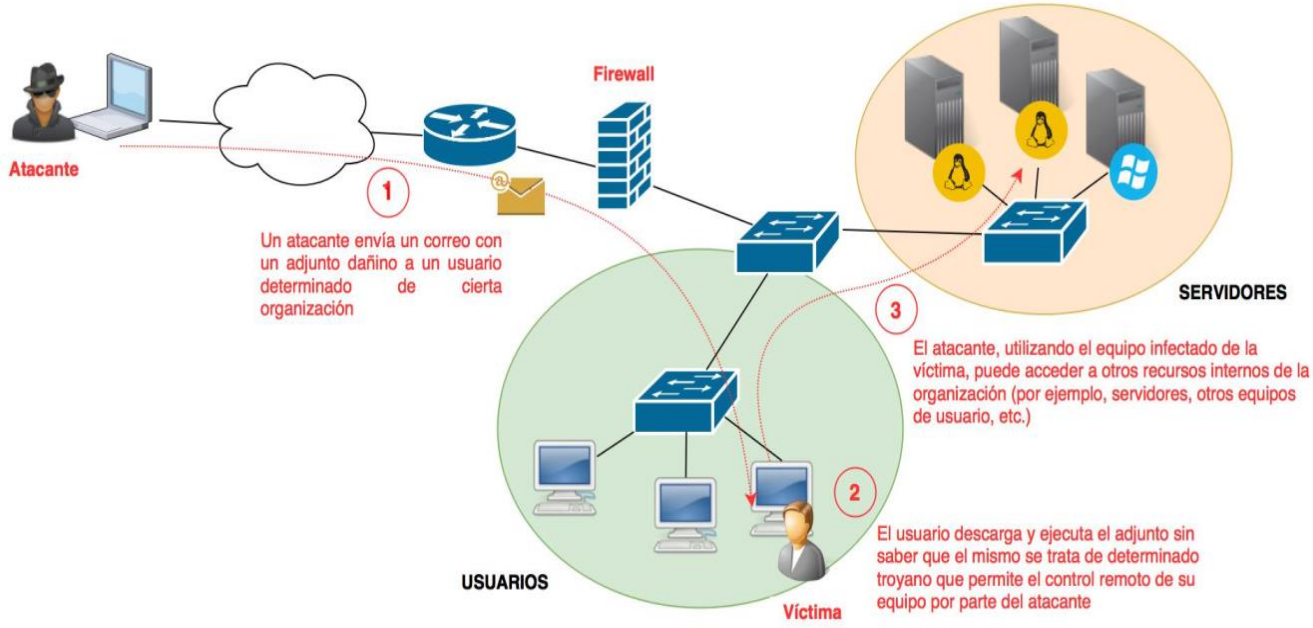
- **Cabeceras** del correo electrónico
- Cuerpo
- Anexos / enlaces



Vector de infección. Correo electrónico

Se requiere de cierto **estudio de la víctima** para perfilar un email más eficaz y creíble.

- Hábitos de navegación, horarios de trabajo, perfiles públicos en redes sociales (LinkedIn, Facebook, etc.), relaciones y alianzas con otras empresas, etc.
- Si el atacante identifica que la organización objetivo "A" tiene ciertas alianzas con la compañía "B", podría elaborar un correo falsificando el remitente y haciéndose pasar por un empleado de la compañía "B".



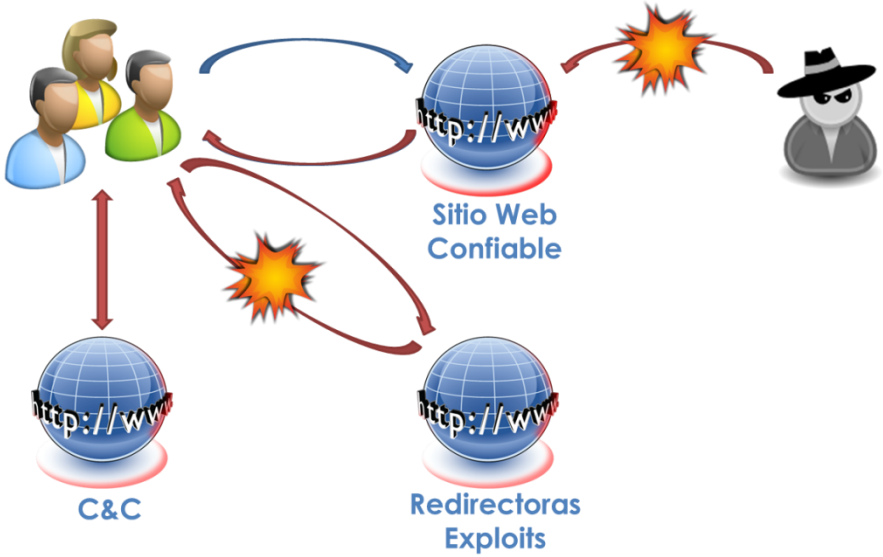
Vector de entrada - Ingeniería social

- Cuidado con los adjuntos
  - **Ejecutable**
    - ¿Realmente alguien sigue ejecutando ficheros .exe desde el correo hoy en día? Solución: RTLO, salvapantallas (.scr)
  - **Word, Excel, PowerPoint**
    - Se debe evitar la apertura de estos ficheros si no estamos seguros completamente del remitente.
    - **Macros!!**
  - **PDF**
    - Se debe evitar la apertura de estos ficheros si no estamos seguros completamente del remitente.

- **¡¡Uso de herramientas corporativas!!**

Vector de infección. Watering Hole (Abrevadero)

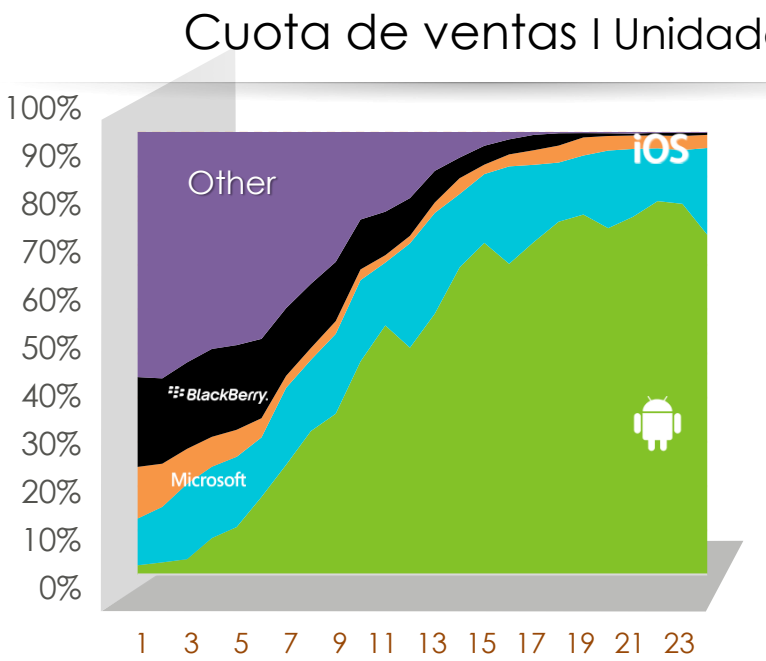
- Ataque a un grupo concreto de usuarios con un interés común donde se **compromete un sitio "confiable"** para todos ellos de manera que, al visitarlo, queden infectadas o se descarguen aplicaciones maliciosas.
- Ataque relacionado con **Drive-by Download Attack:** cualquier tipo de descarga e instalación de software no deseado desde Internet (programas, ActiveX, Java Applets,…) típicamente a través de e-mail, ventanas de pop-up o una página web.



El código dañino (malware) es capaz de las siguientes operaciones:

- Pulsaciones de teclado de registro.
- Captura de audio del micrófono.
- Captura de pantalla.
- Datos de geolocalización.
- Realizar fotos desde la webcam.
- Copiar archivos a un servidor remoto.
- Copia de archivos en un dispositivo USB si está insertado.
- Hijjacking del portapapeles.
- Captura de la información de la máquina de destino.

Telefonía móvil. De diversificación a oligopolio en sistemas operativos



Un riesgo potencial adicional

Posición dominante en

- Preferencias del consumidor
- Plataformas de servicios
- Servicios y aplicaciones
- Dispositivos

Teléfonos móviles. Código dañino

- Código dañino
  - Llamadas entrantes y salientes
  - Mensajes SMS,
  - Ficheros descargados
  - Las coordenadas GPS
  - Mensajería (Whatsapps…)
  - Lista de contactos

≃

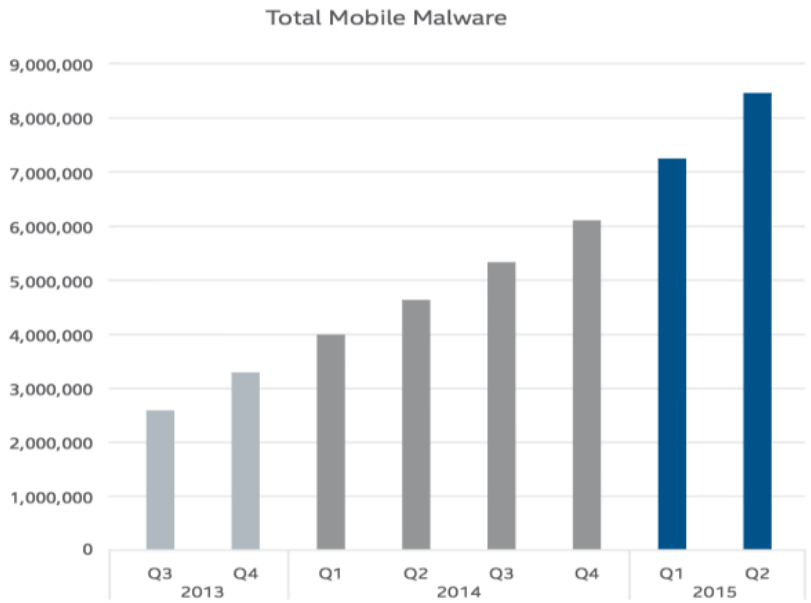
Android Market

Store

PERFECTOS PARA ESPIAR

CCN-CERT_IA-28-15 Seg. Telefonía Móvil

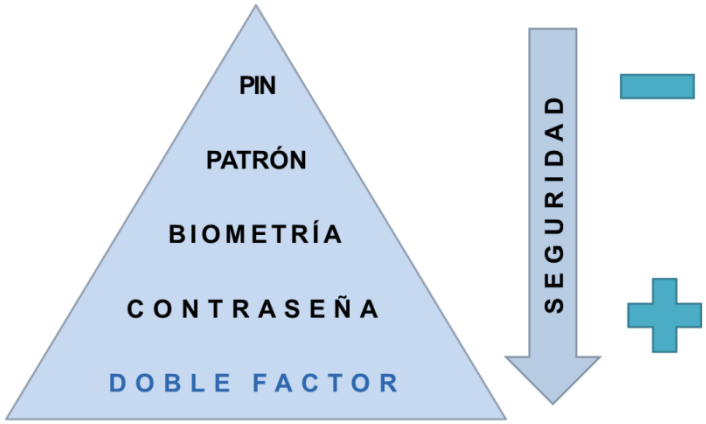
Ejecución remota de código

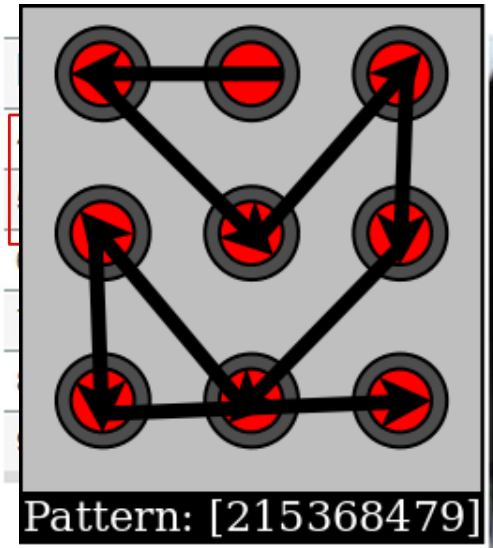


CCN-STIC 450/53/54/55/57

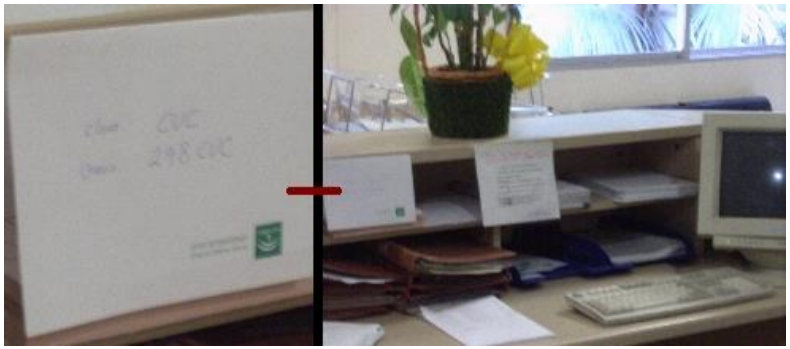
CCN-STIC 827

Cómo de seguro es tu PIN. ¿Dónde lo almacenas?





1234	1234
0000	1111
2580	0000
1111	1212
5555	7777
5683	1004
0852	2000
2222	4444
1212	2222
1998	6969



Ignorancia de buenas prácticas de seguridad y a la **falta de concienciación por parte de los usuarios del Sistema**

Soportes de Información

En los discos duros de los ordenadores hay enormes cantidades de **datos ocultos para los usuarios, pero fácilmente accesibles**. Entre estos datos se encuentran archivos que ingenuamente creemos que hemos borrado, claves de acceso, versiones descifradas de archivos confidenciales y todo tipo de rastros sobre la actividad del equipo.

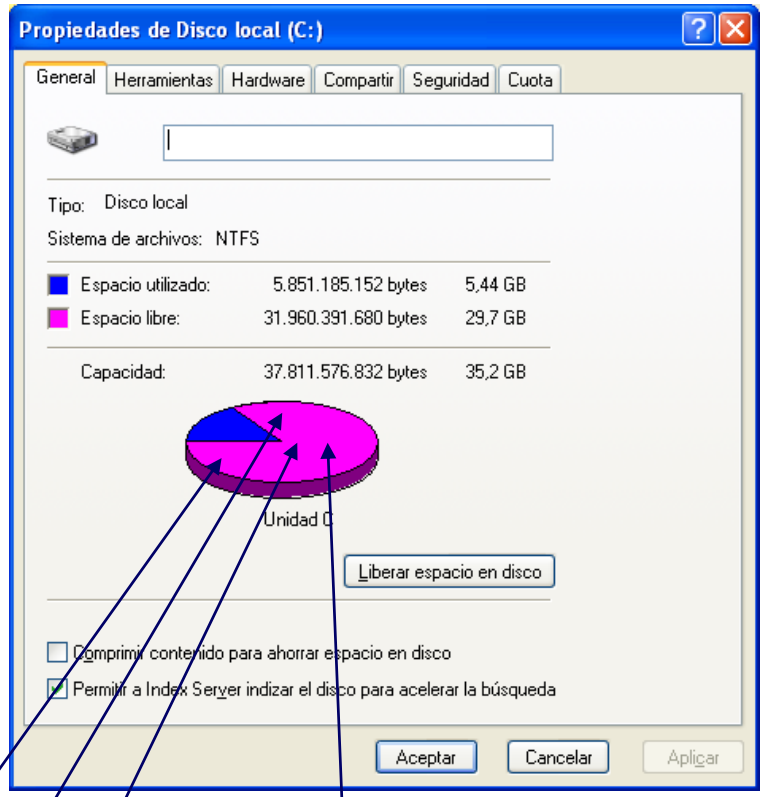
¡Cuidado con las copias sin cifrar!

Usar unidades de red

COMPRIMIR……. CON WINRAR

BORRAR…….. CON ERASER

CIFRAR …….CON PGP



Número de tarjeta de crédito

Copias en legibles de los documentos cifrados

Los registros temporales con datos de clientes

Claves de acceso a sitios seguros

Herramientas para Android

CCNDroid Wiper.
borrado seguro de ficheros.

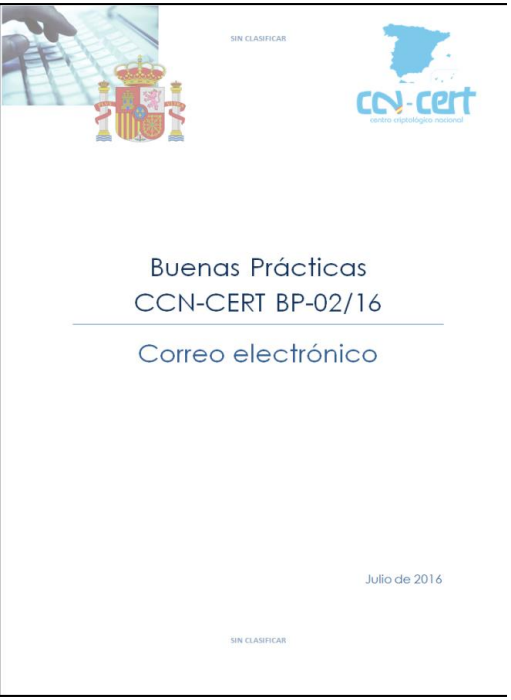
CCNDroid Crypter.
cifrado de ficheros con distintos algoritmos

www.ccn-cert.cni.es

RECOMENDACIONES

- CCN-CERT_BP-02-16_Correo_electrónico.
- CCN-CERT IA-28-15 Medidas de seguridad en telefonía móvil.
- www.ccn-cert.cni.es

Guía de Buenas Prácticas



	Decálogo de seguridad del correo electrónico
1	No abra ningún enlace ni descargue ningún fichero adjunto procedente de un correo electrónico que presente cualquier síntoma o patrón fuera de lo considerado normal o habitual.
2	No confíe únicamente en el nombre del remitente. El usuario deberá comprobar que el propio dominio del correo recibido es de confianza. Si un correo procedente de un contacto conocido solicita información inusual contacte con el mismo por teléfono u otra vía de comunicación para corroborar la legitimidad del mismo.
3	Antes de abrir cualquier fichero descargado desde el correo asegúrese de la extensión y no se fíe por el icono asociado al mismo.
4	No habilite las macros de los documentos ofimáticos incluso si el propio fichero así lo solicita.
5	No debe hacerse clic en ningún enlace que solicite datos personales ni bancarios.
6	Tenga siempre actualizado el sistema operativo, las aplicaciones ofimáticas y el navegador (incluyendo los plugins/extensiones instalados).
7	Utilice herramientas de seguridad para mitigar *exploits* de manera complementaria al software antivirus.
8	Evite hacer clic directamente en cualquier enlace desde el propio cliente de correo. Si el enlace es desconocido es recomendable buscar información del mismo en motores de búsqueda como Google o Bing.
9	Utilice contraseñas robustas para el acceso al correo electrónico. Las contraseñas deberán ser periódicamente renovadas. Si es posible utilice doble autenticación.
10	Cifre los mensajes de correo que contengan información sensible.

1. Aumentar la capacidad de Vigilancia.
2. Herramientas de Gestión Centralizada.
3. Política de seguridad.
4. Aplicar configuraciones de seguridad.
5. Empleo de productos confiables y certificados.
6. Concienciación de usuarios.
7. Compromiso de dirección (Aceptación Riesgo)
8. Legislación y Buenas Prácticas.
9. Intercambio de Información.
10. Trabajar como si se estuviera comprometido.

CONCLUSIONES

- Incremento constante del **número, sofisticación y complejidad** de los **ciberataques**
- **El ciberespionaje** sobre las administraciones públicas y las empresas estratégicas **es la amenaza más importante** para los intereses nacionales y la seguridad nacional
- La **dificultad de atribución** es el factor que caracteriza esta amenaza en relación con otras.
- La **amenaza procede** tanto de países con intereses encontrados como de países con intereses afines (¿amigos?).
- Es preciso reforzar la capacidad de **prevención y protección** en todas las instancias del Estado (ciudadanos, empresas y administraciones públicas)
- Es preciso reforzar las **capacidades de INTELIGENCIA y de PERSECUCIÓN DEL DELITO TECNOLÓGICO** para la identificación de atacantes, determinación de sus objetivos y aplicar la legislación vigente al respecto.

Invertir en CIBERSEGURIDAD al menos una cantidad equivalente que en SEGURIDAD FÍSICA.

¿PREGUNTAS?

La **"huella digital" de nuestra vida, consciente o desapercibida, tendrá un enorme valor económico en el futuro,** y se podrá vender e intercambiar por efectivo, descuentos, productos o servicios que cada vez están más personalizados y adaptados al cliente.

- **E-Mails**
  - **ccn-cert@cni.es**
  - **info@ccn-cert.cni.es**
  - **ccn@cni.es**
  - sat-inet@ccn-cert.cni.es
  - sat-sara@ccn-cert.cni.es
  - **incidentes@ccn-cert.cni.es**
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - **www.ccn-cert.cni.es**
  - www.oc.ccn.cni.es

Gracias