Deloitte.

Ciberseguridad
Un nuevo contexto de amenazas para la administración electrónica

Daniel Madrid
13/04/2015

Deloitte.

Copia distribuida para uso exclusivo del Govern Balear para su proyección durante la 5ª Jornada de Administración Electrónica.

Queda prohibida la reproducción, distribución, comunicación a terceros, transformación, total o parcial, gratuita u onerosa, por cualquier medio o procedimiento, sin la autorización previa y por escrito de Deloitte Advisory S.L.

Este documento es estrictamente confidencial.

Índice

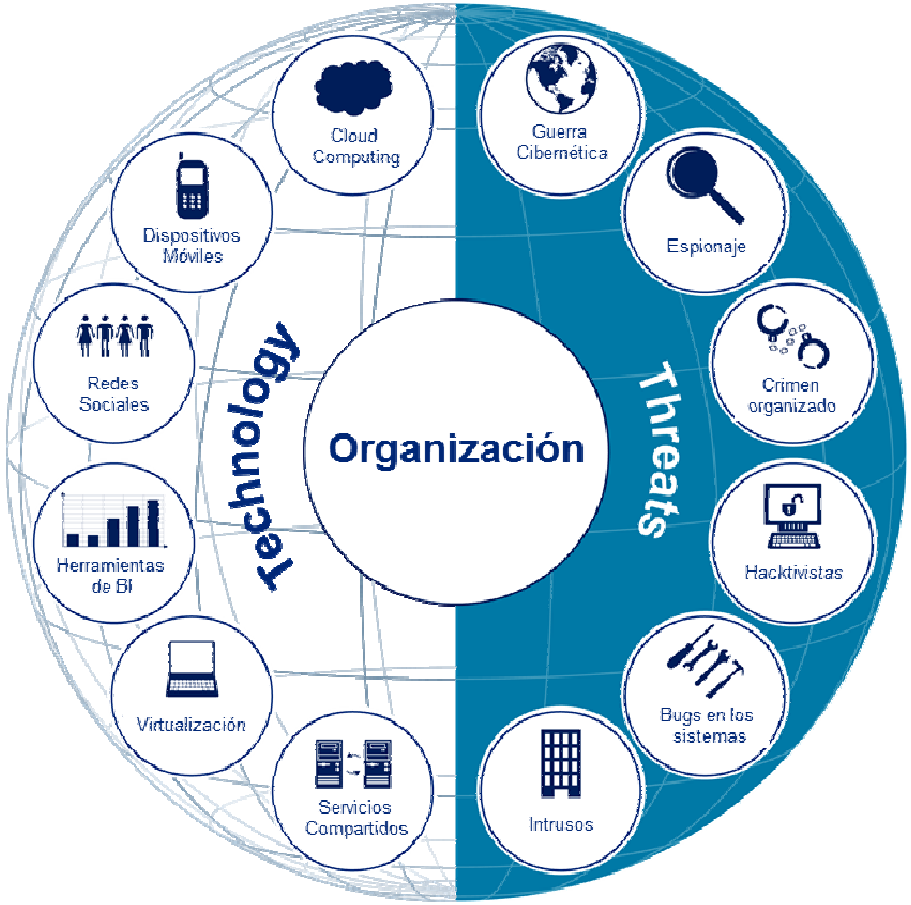
Un nuevo contexto

Hace dos años…

http://www.deloitte.com/view/en_GB/uk/market-insights/cyber-security/

Un nuevo contexto

… riesgos en un mundo hiperconectado…



La revolución digital está generando nuevos modelos de relación:

- Entre administración y los ciudadanos (G2C)
- Entre administraciones (G2G)
- Entre la administración y sus empleados (G2E)

pero también genera un escenario con **nuevos riesgos que deben ser identificados y evaluados para poder promover y desarrollar una aproximación coherente de protección.**

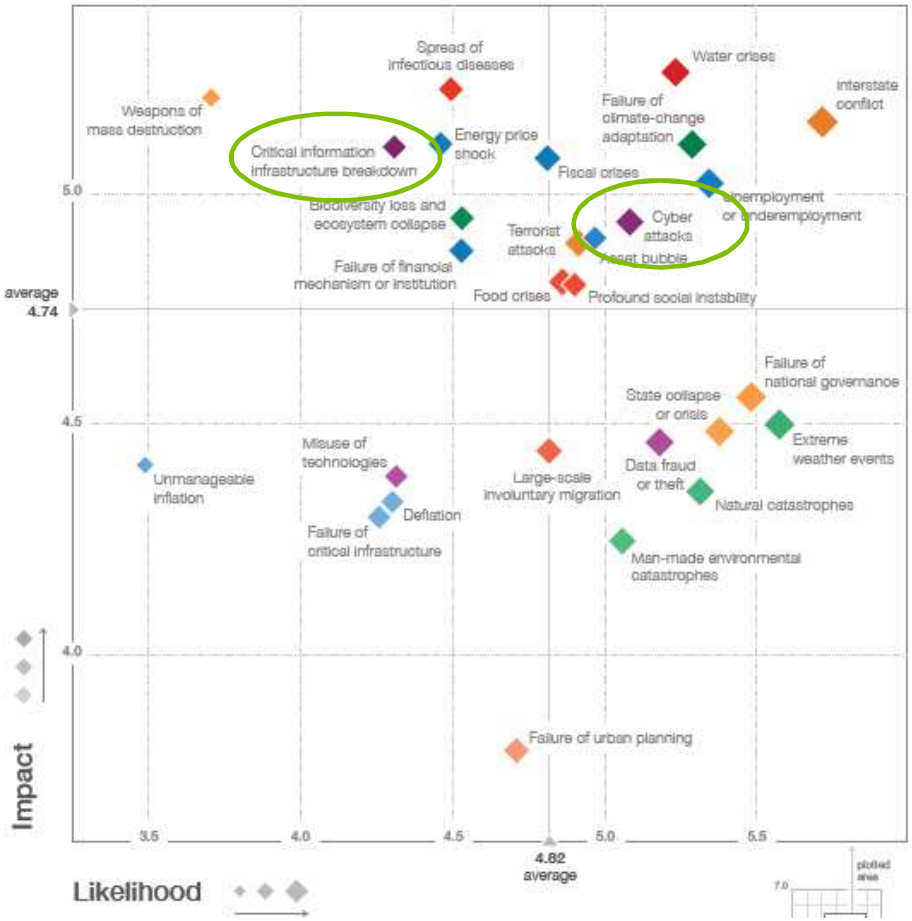
Un nuevo contexto

… con innumerables amenazas …

Un nuevo contexto

… que generan un impacto real …

Fuente: WEF Global Risk Report 2015



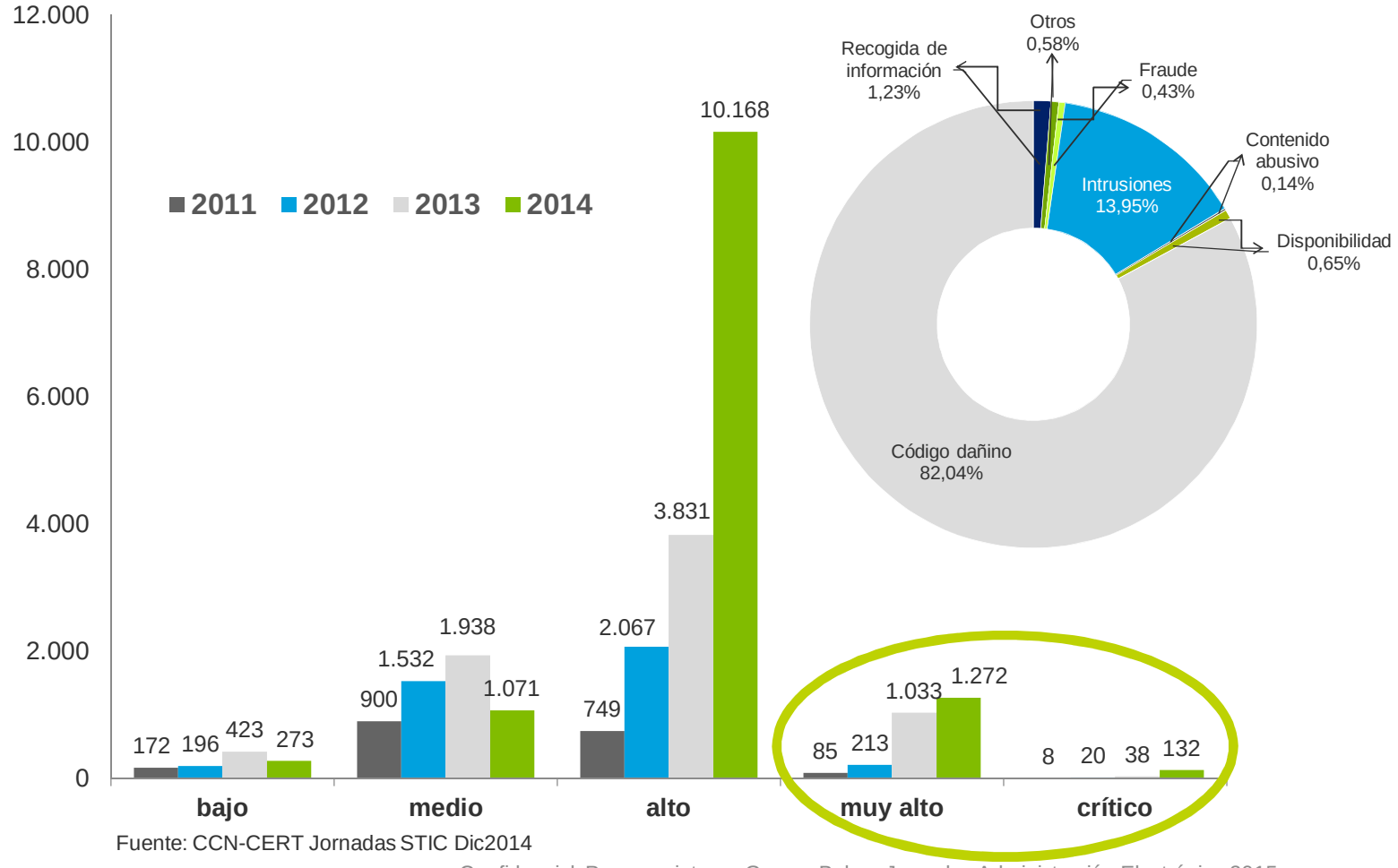
"Global interconnectedness and the rising speed of information transmission have reinforced the interdependence between geopolitics and economics, with ***cyberspace representing an important new front*** *in the geopolitical equation as* ***cyber attacks have the growing potential to inflict economic damage****"*

WORLD ECONOMIC FORUM

"2015 differs markedly from the past, with ***rising technological risks, notably cyber attacks,*** *and new economic realities, which remind us that geopolitical tensions present themselves in a very different world from before."*

Un nuevo contexto

… también para las administraciones públicas …



Fuente: CCN-CERT Jornadas STIC Dic2014

Un nuevo contexto

… qué ha cambiado?

El paso de la seguridad de la información...

Desaparición del perímetro

…a la ciberseguridad…

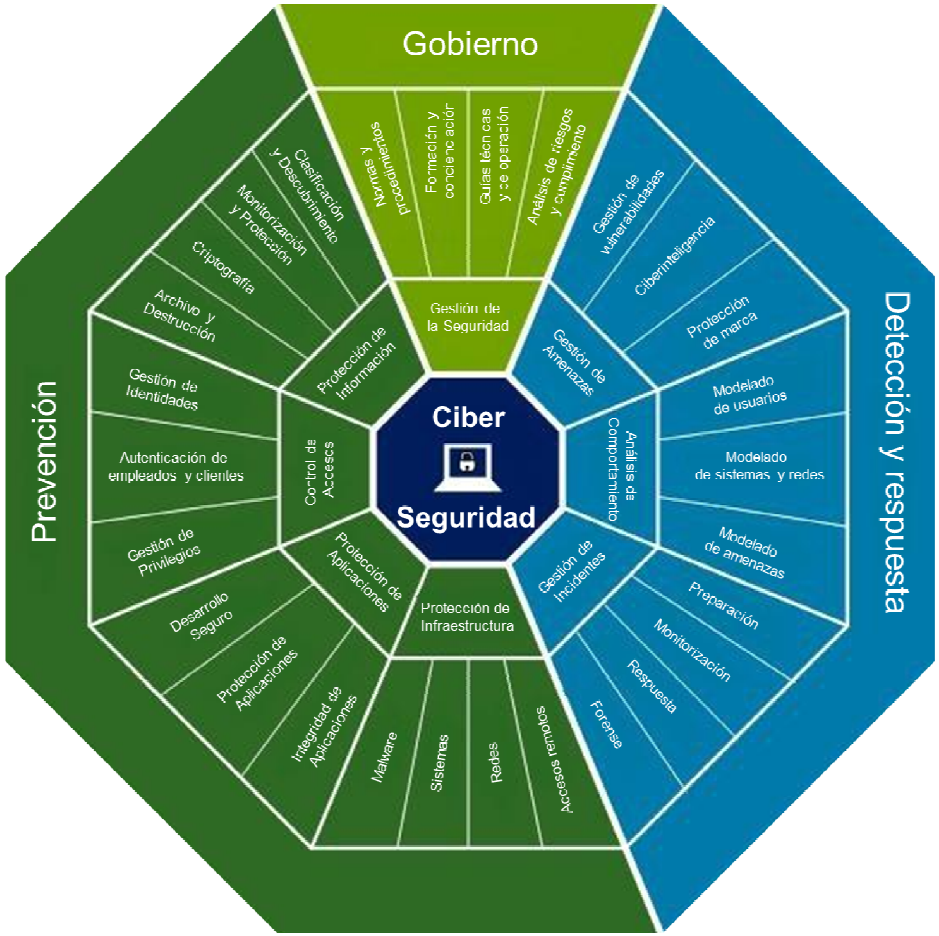
La importancia de los tiempos

…requiere de nuevas capacidades

El impacto sobre la reputación

Un nuevo contexto

… qué debemos cambiar?



P **Preparar** la Organización para gestionar adecuadamente los riesgos de ciberseguridad implantando estructuras de gobierno que permitan mantener las capacidades de cíberseguridad.

D **Defender la** Organización frente a ciberataques manteniendo las inversiones y mejorando las medidas para proteger sus activos de información digitales.

A **Anticipar** la identificación de las amenazas mediante el uso de las múltiples fuentes de ciberinteligencia con el fin de poder gestionarlas proactivamente.

R **Responder** anticipadamente ante un ciberataque existoso**,** con el fin de poder limitar su impacto sobre la Organización.

Índice

Contexto: ciberamenazas y ciberseguridad

Cómo debemos actuar

Un ejemplo práctico: @clave

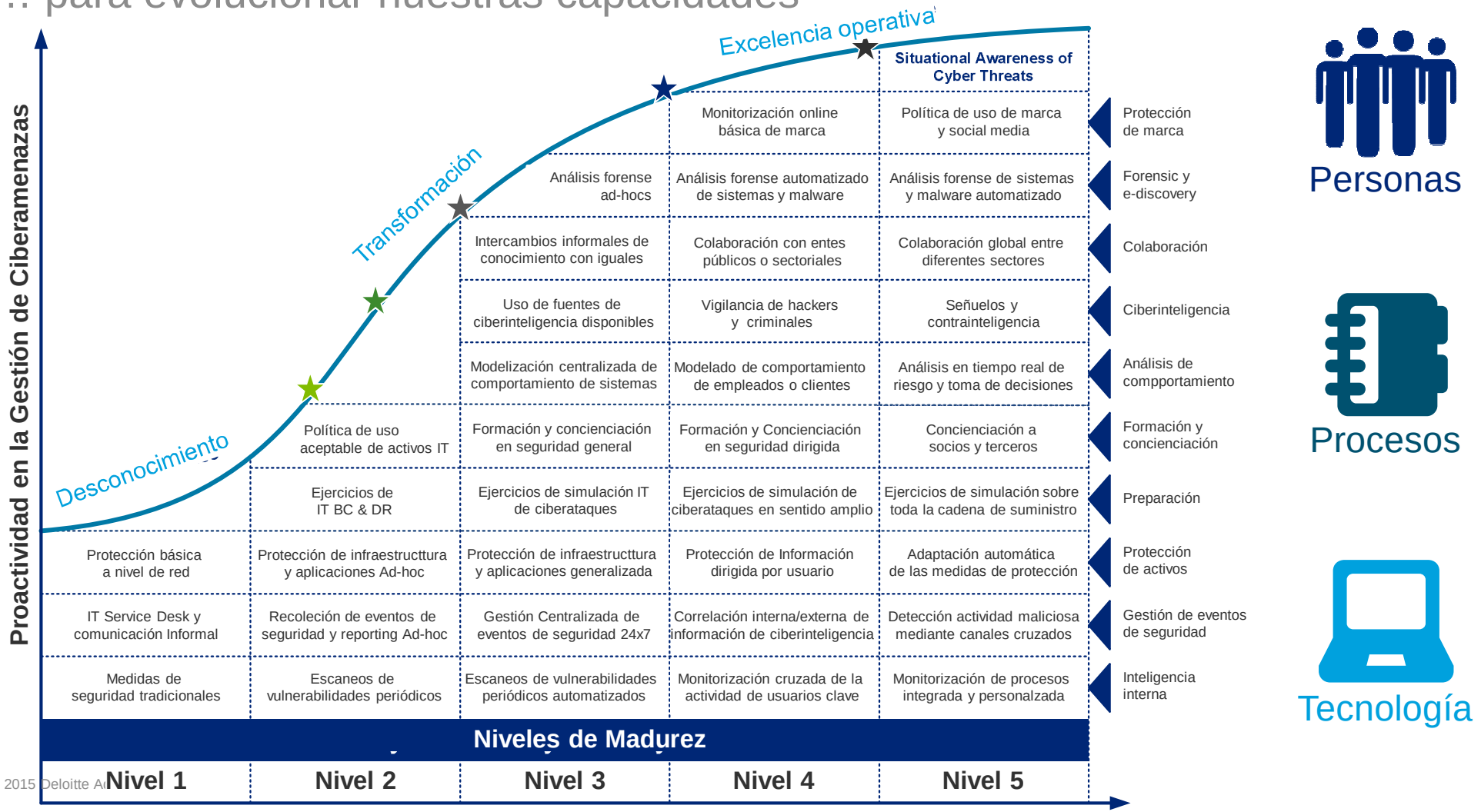
Conclusiones

Cómo debemos actuar

Caracterizar las amenazas…

Cómo debemos actuar

… para evolucionar nuestras capacidades



Personas

Procesos

Tecnología

Índice

Contexto: ciberamenazas y ciberseguridad

Cómo debemos actuar

Un ejemplo práctico: @clave

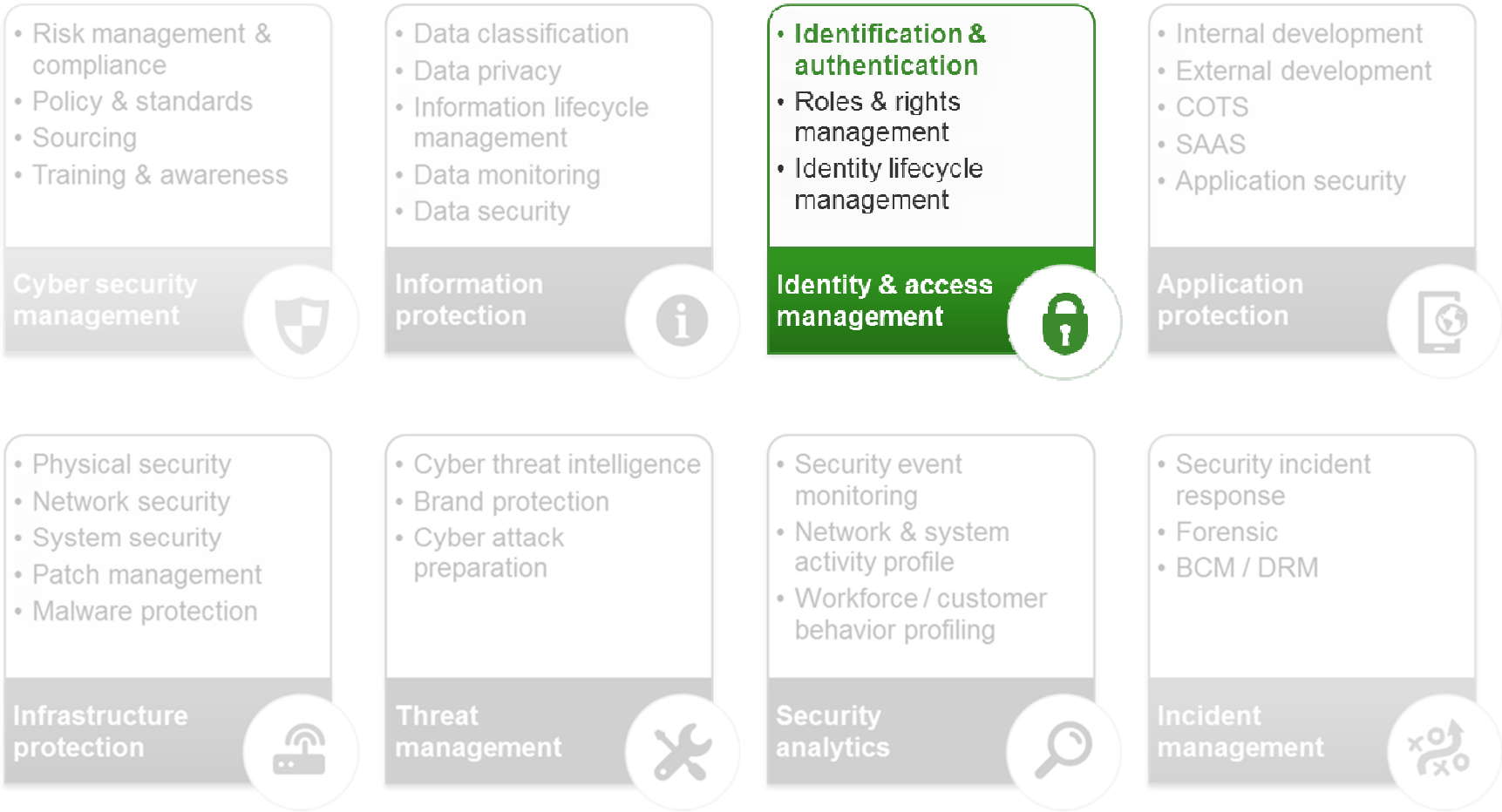
Conclusiones

Un ejemplo práctico

Una de las capacidades básicas: Gestión de identidades y accesos

Un ejemplo práctico

Una de las capacidades básicas: Gestión de identidades y accesos



Un ejemplo práctico

¿Por qué es necesario reforzar esta capacidad?

EXPANSION 30

30 PROMESAS: EL TALENTO QUE TRANSFORMARÁ A MÉXICO
Edición 1162
SUSCRÍBETE

CNN EXPANSIÓN

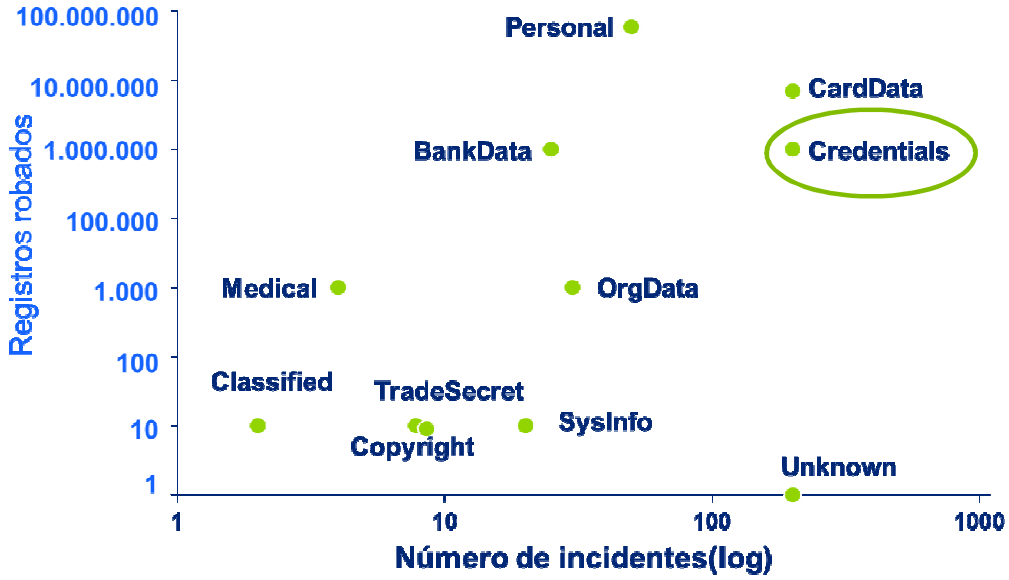
Inicio | Empresas | Economía | Mercados | Finanzas Personales | Emprendedores | Carrera | Tecnología | Videos

Las 25 peores contraseñas del 2014

'123456' y 'qwerty' se mantienen en los primeros lugares del registro elaborado por SplashData; para elaborar un código seguro se recomienda mezclar letras y números.

Miércoles, 21 de enero de 2015 a las 10:35

1. 123456
2. password
3. 12345
4. 12345678
5. qwerty
6. 123456789
7. 1234
8. baseball
9. dragón
10. football



Mecanismo de autenticación [op.acc.5]

		Nivel		
		BAJO	MEDIO	ALTO
algo que se sabe	claves concertadas	sí	Con cautela	no
algo que se tiene	Tokens	si	sí	criptográficos
algo que se es	Biometría	sí	sí	+ doble factor

Un ejemplo práctico
@clave

IDENTIDAD ELECTRÓNICA PARA LAS ADMINISTRACIONES

Plataforma común para la identificación, autenticación y firma electrónica que:

Evita a las Administraciones Públicas tener que implementar y gestionar sus propios sistemas de identificación y firma.

Evita a los ciudadanos tener que utilizar métodos de identificación diferentes para relacionarse electrónicamente con la Administración.

Permite definir el nivel de aseguramiento en la calidad de la autenticación que desean (nivel QAA), en base a la clasificación de seguridad definida de acuerdo al ENS (Real Decreto 3/2010).

Un ejemplo práctico
@clave

IDENTIDAD ELECTRÓNICA PARA LAS ADMINISTRACIONES

Cl@ve contempla la utilización de sistemas de identificación basados en claves concertadas con dos posibilidades de uso:

- Cl@ve ocasional (Cl@ve PIN): sistema de contraseña de validez muy limitada en el tiempo, orientado a usuarios que acceden esporádicamente a los servicios, que se corresponde con el sistema PIN24H de la AEAT.
- Cl@ve permanente: sistema de contraseña de validez duradera en el tiempo, pero no ilimitada, orientado a usuarios habituales. Se corresponde con el sistema de acceso mediante usuario y contraseña, reforzado con claves de un solo uso por SMS, a los servicios de Tu Seguridad Social. Este sistema será además el que permitirá el acceso al ciudadano a la firma en la nube.

Cl@ve contempla adicionalmente el uso de certificados electrónicos (incluyendo el DNI-e).

4,3%

Utilización del DNIe en sus trámtites con las AAPPs

13,1%

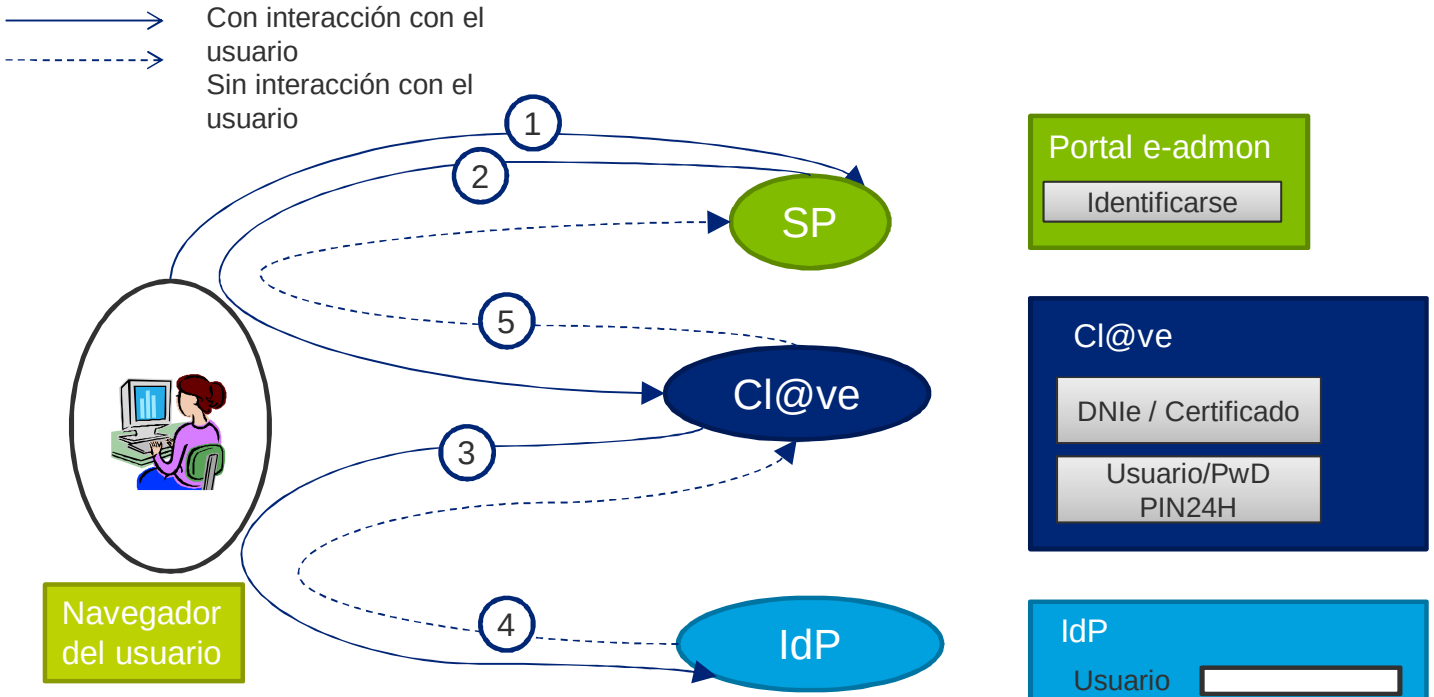
Utilización de otros certificados digitales en sus trámtites con las AAPPs

41,5%

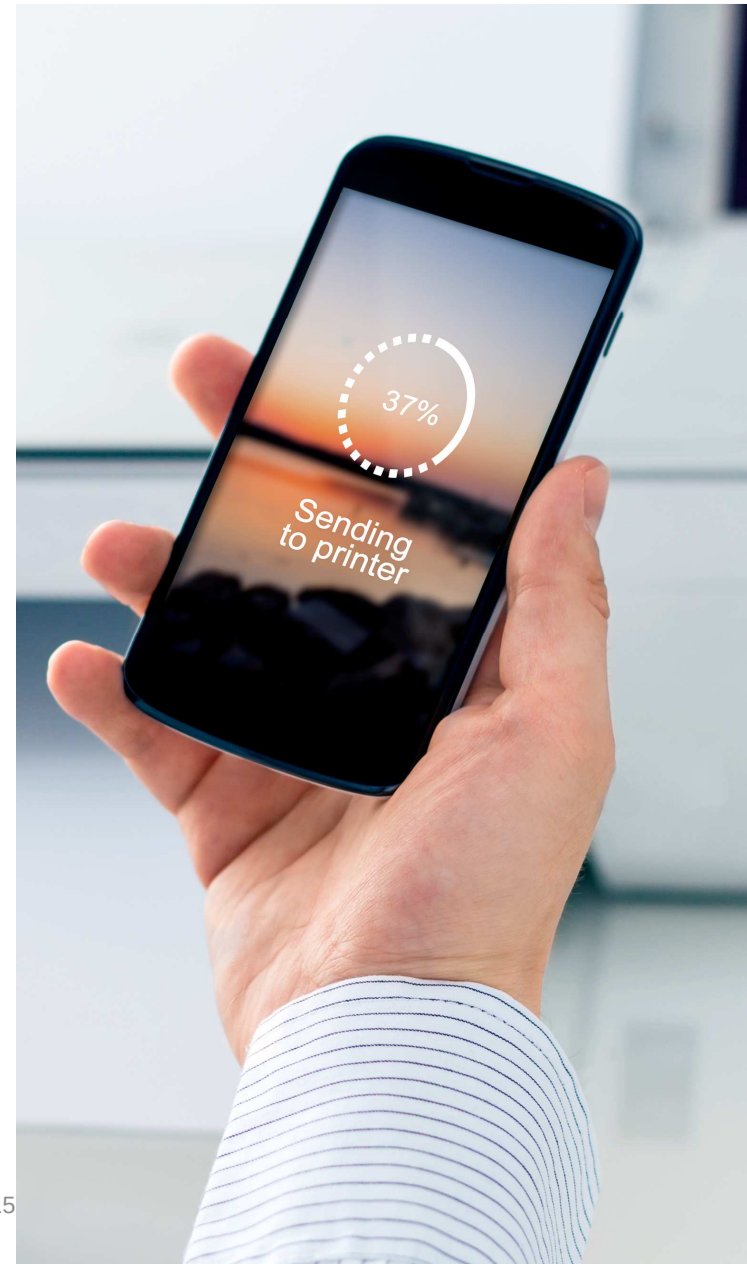
Declaraciones de la renta presentadas telemáticamente (PIN24H)

Un ejemplo práctico

@clave



Mensajes SAML
2 - Servicio que invoca (SP), nivel de calidad de eID exigido, firmado por SP
3 - Servicio que invoca (SP), nivel de calidad de eID, firmado por Cl@ve
4 – Respuesta de la identificación, firmada por IdP
5 – Respuesta de la identificación, firmada por Cl@ve



Índice

Contexto: ciberamenazas y ciberseguridad

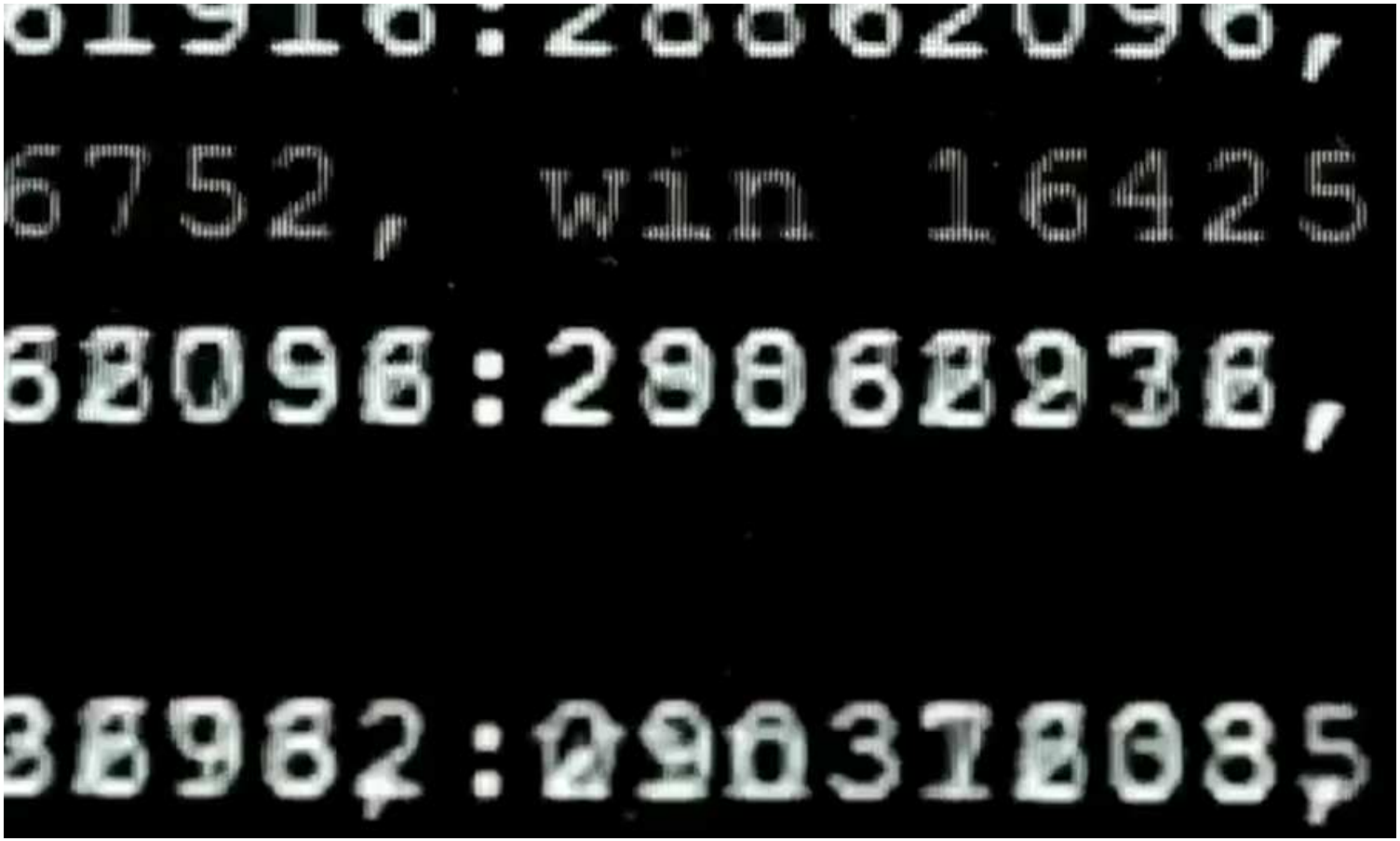
Cómo debemos actuar

Un ejemplo práctico: @clave

Conclusiones

Conclusiones

Un ejercicio práctico



Deloitte hace referencia, individual o conjuntamente, a Deloitte Touche Tohmatsu Limited ("DTTL"), sociedad del Reino Unido no cotizada limitada por garantía, y a su red de firmas miembro y sus entidades asociadas. DTTL y cada una de sus firmas miembro son entidades con personalidad jurídica propia e independiente. DTTL (también denominada "Deloitte Global") no presta servicios a clientes. Consulte la página www.deloitte.com/about si desea obtener una descripción detallada de DTTL y sus firmas miembro.

Deloitte presta servicios de auditoría, consultoría, asesoramiento fiscal y legal y asesoramiento en transacciones y reestructuraciones a organizaciones nacionales y multinacionales de los principales sectores del tejido empresarial. Con más de 200.000 profesionales y presencia en 150 países en todo el mundo, Deloitte orienta la prestación de sus servicios hacia la excelencia empresarial, la formación, la promoción y el impulso del capital humano, manteniendo así el reconocimiento como la firma líder de servicios profesionales que da el mejor servicio a sus clientes.