Foro de Transformación Digital de la Justicia

Foro de Transformación Digital de la Justicia

GRUPO DE TRABAJO

Ciberseguridad

Secretaría General para la Innovación y Calidad del Servicio Público de Justicia

Abril 2022

GOBIERNO DE ESPAÑA MINISTERIO DE JUSTICIA

SECRETARÍA DE ESTADO DE JUSTICIA

SECRETARÍA GENERAL PARA LA INNOVACIÓN Y CALIDAD DEL SERVICIO PÚBLICO DE JUSTICIA

AGENDA 2030

ÍNDICE

01. El Subcomité de seguridad - ¿Por qué el Subcomité de Seguridad de CTEAJE? (I)

CUMPLIR CON LA NORMATIVA

Ley 18/2011, de 5 de julio, **reguladora del uso de las tecnologías** de la información y la comunicación en la Administración de Justicia.

ES UN ESCENARIO COMPLEJO

En proceso de transformación digital. **multitud de actores.**

NECESIDAD DE RACIONALIZACIÓN Y ORGANIZACIÓN

Aprobación de **la PSI de la Administración Judicial Electrónica.**

¿QUÉ PERSIGUE?

- Alcanzar la **madurez necesaria en ciberseguridad** en la Administración de Justicia.

¿CÓMO LO CONSEGUIRÁ?

- Basándose en el **cumplimiento del Esquema Nacional de Seguridad.**
- Y aportando los **elementos facilitadores para el desarrollo** de la **Política de Seguridad de la Administración Judicial Electrónica.**

¿CÓMO SE VA A GOBERNAR?

- Mediante el órgano especializado de **CTEAJE**, el **Subcomité de Seguridad.**

El **Subcomité de Seguridad** es el **órgano especializado y permanente** para la **seguridad judicial electrónica** creado en el seno del **Comité Técnico Estatal de la Administración Judicial Electrónica** de conformidad con la Política de Seguridad de la Información de la **Administración Judicial Electrónica.**

CTEAJE

Art. 8. Coordinación de las acciones derivadas del cumplimento de la PSIJE del CTEAJE

*Se crea el **Subcomité de Seguridad** como un **órgano especializado y permanente para la seguridad judicial electrónica en el seno del CTEAJE**, integrado por aquellas personas con **responsabilidad en materia de seguridad** de cada una de las instituciones integrantes o en su caso por aquellos designados en representación de cada Comité de Seguridad de la Información, así como por las personas que se designe por el CGPJ y la FGE."*

El nuevo modelo de organización y funcionamiento del Subcomité deberá tener en consideración las premisas que siguen:

Contribuir

de forma relevante a la **transformación del Servicio Público de Justicia,** garantizando la seguridad jurídica digital mediante la innovación y desarrollo de buenas prácticas y la normativa necesaria para la implantación efectiva del **Esquema judicial de interoperabilidad y seguridad.**

Promover

activamente el **cogobierno de la seguridad jurídica digital** con las CCAA y otras instituciones, evitando ineficacias, duplicidades, solapamientos, descoordinación o conflictos en el diseño, desarrollo, despliegue y operación de los **sistemas de información de la Administración de Justicia.**

01. El Subcomité de seguridad - Funciones y capacidades (V)

FUNCIONES

- Desarrollar y mantener un **marco común organizativo y colaborativo** en materia de seguridad para los sistemas informáticos y de comunicaciones de Administración de Justicia.
- Definir los procedimientos operativos y de coordinación del Subcomité.
- Desarrollar y mantener un marco común de **indicadores y analítica de datos**.
- Establecimiento y seguimiento de **objetivos comunes** de seguridad y cumplimiento.
- **Mejora continua** del proceso de seguridad.
- **Intercambio de experiencias**, conocimiento, herramientas y casos de éxito con CCAA y otros organismos.
- Integración con otros marcos de gobernanza de **ámbito europeo**.

CAPACIDADES

- **Portal de Gobernanza de la Seguridad del Servicio Público de Justicia.**
- **Realización de informes anuales del estado de la seguridad, técnicos, de incidentes, mejoras y ad-hoc.**
- **Repositorio de experiencias, conocimiento, herramientas y casos de éxito.**
- **Implantación y provisión de herramientas de comunicación y colaboración.**
- **Implantación y provisión de herramientas de evaluación del estado de seguridad (INES).**
- **Implantación y provisión de herramientas de analítica de datos.**

FUNCIONES

- Actualización, mantenimiento y distribución de la **Política de Seguridad de la Información de la Administración Judicial Electrónica (PSIJE) y normativa** del Esquema judicial de interoperabilidad y seguridad.
- Integración con normativa y de buenas prácticas de **ámbito europeo.**
- **Coordinación con Grupos de Trabajo** CTEAJE, CCAA y otros organismos.
- **Aprobación de la normativa** de 2 º y de 3º nivel, en su caso.
- **Mejora continua e innovación del cuerpo normativo** del Esquema judicial de interoperabilidad y seguridad.

CAPACIDADES

- **Oficina de Desarrollo Normativo.**
- **Traducción a lenguas cooficiales.**
- **Implantación y provisión de herramientas (AMPARO).**
- **LAB de innovación en buenas prácticas y herramientas.**
- **(Espacio creativo, de colaboración público-privada y abierto para la adaptación de la normativa y sus herramientas a las tecnologías disruptivas habilitadoras (IA, Blockchain, …)**

FUNCIONES

- Desarrollar y mantener un **marco común** de análisis y tratamiento de **amenazas y riesgos** para todos los sistemas de información de la Administración de Justicia.

- Desarrollar y mantener un **marco común** de análisis y tratamiento de **amenazas y riesgos** para los tratamientos de **datos personales** de los sistemas de información la Administración de Justicia.

- Establecimiento de **Requisitos y Niveles** comunes de seguridad para los sistemas de información de la Administración de Justicia.

- **Seguimiento de planes de tratamiento** de riesgos.

CAPACIDADES

- **Catalogo de elementos, amenazas y técnicas (MAGERIT Versión Administración de Justicia).**

- **Repositorio de amenazas y salvaguardas para los Sistemas de Información de la Administración de Justicia (Categoría Básica, Media, Alta).**

- **Foro de DPD.**

- **Traducción a lenguas cooficiales.**

- **Implantación y provisión de herramientas (PILAR).**

FUNCIONES

- **Gestión federada** con CCAA y otros organismos.
- **Integración con CERTs** de ámbito nacional y europeo.
- Coordinación de actuaciones ante **incidentes críticos** de ámbito estatal.
- Análisis de incidentes.
- **Coordinación** con CCN y otros **agentes** (FCS, INCIBE, CNPIC) y contacto con las autoridades de control (CGPJ, AEPD, Agencias de protección de datos de las CCAA).

CAPACIDADES

- **Centro de Operaciones de Ciberseguridad para la Administración de Justicia (COCS-AJE).**
- **Procedimientos de recogida y consolidación de la información, coordinación, operación, comunicación y respuesta.**
- **Federación de SOC´s de CCCA y otros organismos.**
- **Implantación y provisión de herramientas (LUCIA) y de sondas.**
- **Laboratorio de Ciberinteligencia, respuesta y análisis forense.**

FUNCIONES

- Desarrollar y mantener un **esquema común de evaluación, auditoría y certificación** para sistemas de información de la Administración de Justicia.
- Establecimiento de **criterios comunes** de Categorización, Declaración de aplicabilidad, etc. para los sistemas de información de la Administración de Justicia.
- Coordinación con CCN y otras entidades de certificación.
- Integración con otros marcos de certificación de ámbito europeo (ENISA).

CAPACIDADES

- **Órgano Técnico de Certificación de la conformidad con el EJIS.**
- **Catalogo de Perfiles de Cumplimiento para sistemas de información de la Administración de Justicia.**
- **Registro de certificaciones de sistemas y organismos.**
- **Registro de Auditores y entidades de certificación.**
- **Implantación y provisión de herramientas de auditoría.**
- **Laboratorio de auditoría técnica.**

FUNCIONES

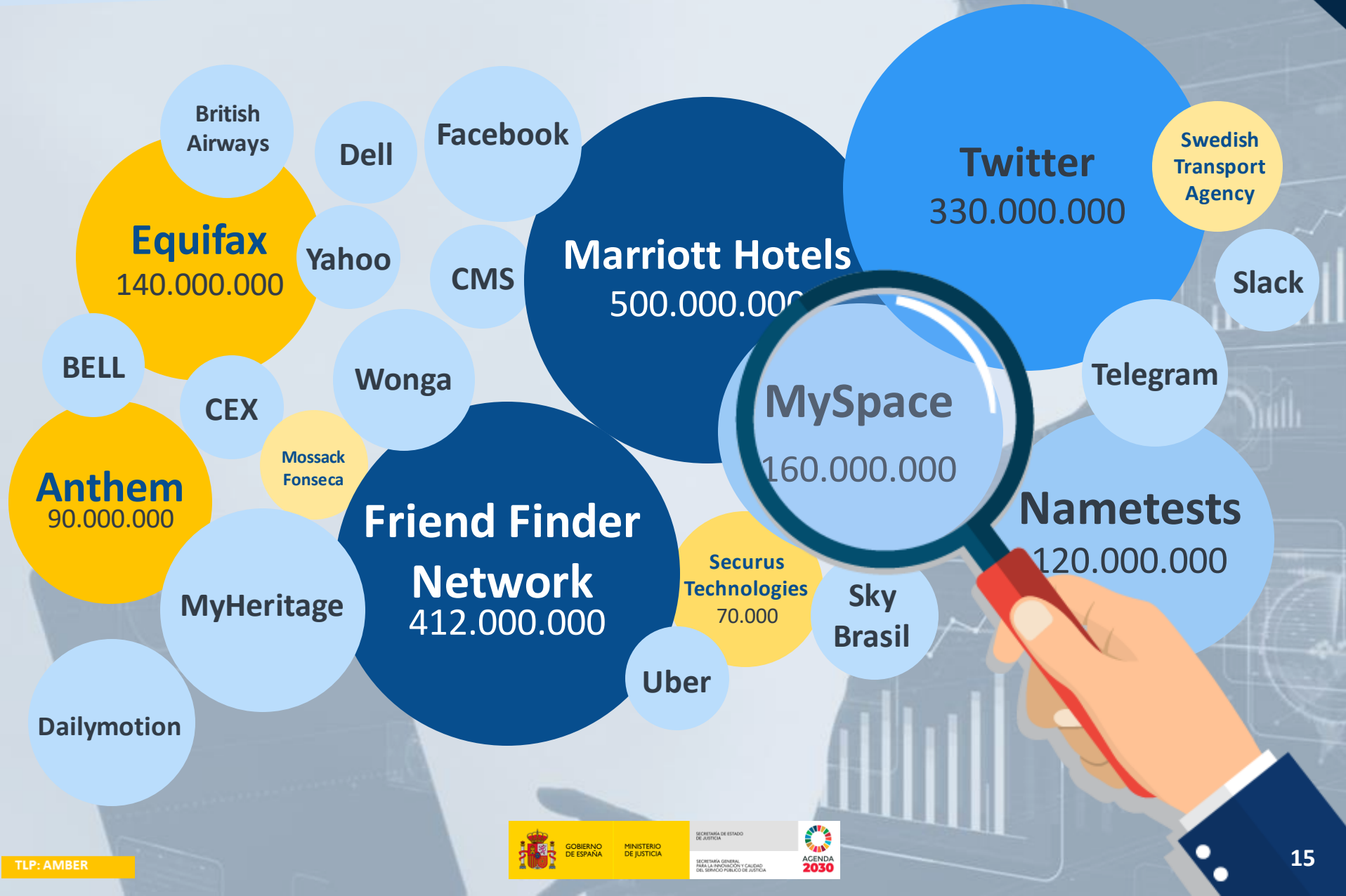
- Desarrollar y mantener un **marco común** de formación y concienciación en materia de seguridad y protección de datos personales.
- Promover un **esquema de evaluación y certificación de conocimientos** de usuarios y técnicos de la Administración de Justicia.
- **Coordinación** con Universidades, Centro de Estudios Jurídicos, Escuela Judicial del CGPJ, entidades de formación y de certificación.
- Integración con otros marcos de formación continua y certificación profesional de ámbito europeo.

CAPACIDADES

- **Plataforma de Formación de la Seguridad del Servicio Público de Justicia.**
- **Repositorio de cursos, píldoras, webinars, casos, etc.**
- **Traducción a lenguas cooficiales.**
- **Implantación y provisión de herramientas (ÁNGELES).**
- **Registro de evaluaciones y certificaciones de conocimientos de usuarios y técnicos.**

ÍNDICE

02. Las autoridades de control de protección de datos (I)



02. Las autoridades de control de protección de datos (II)

MARCO NORMATIVO

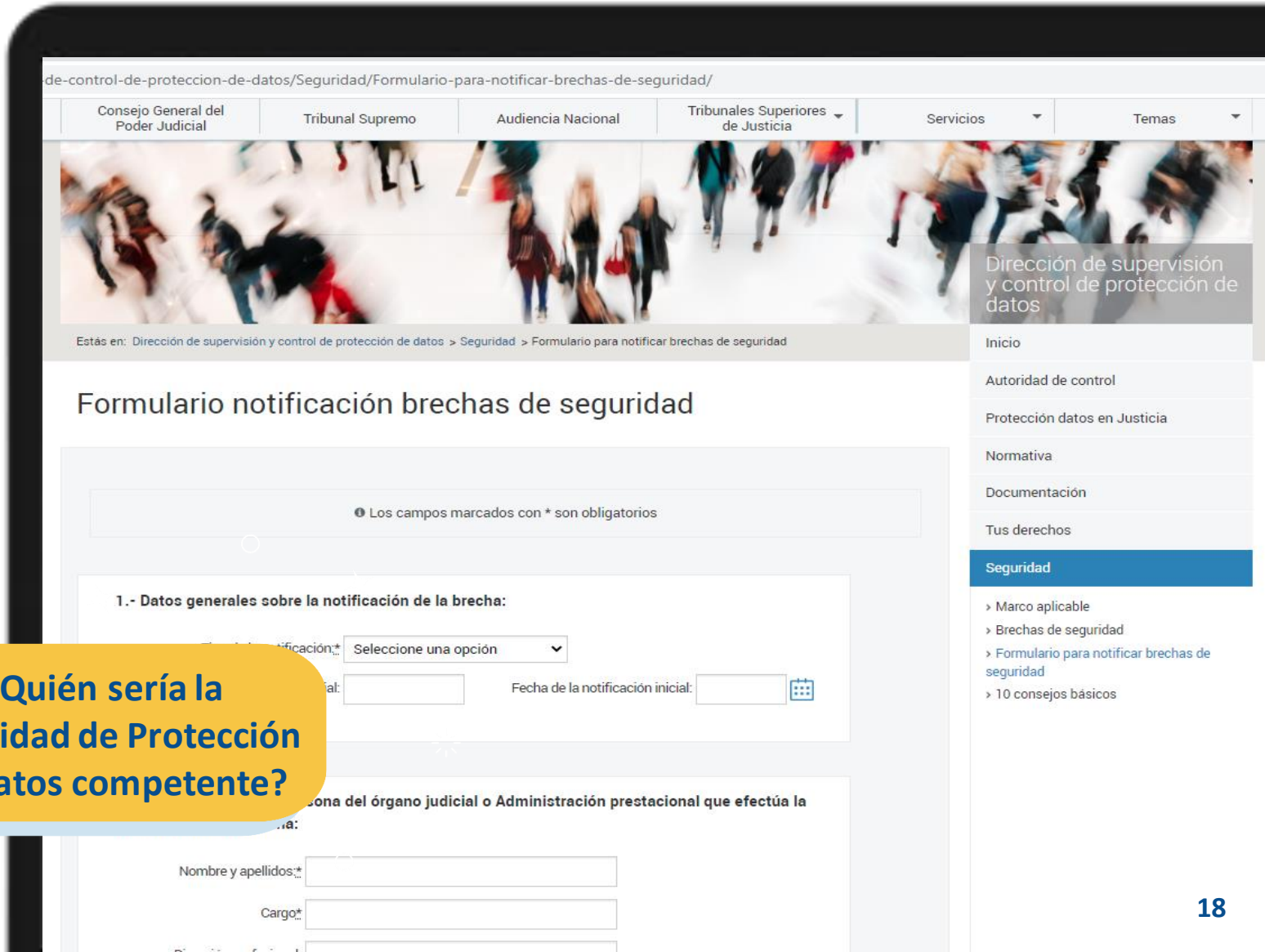
Reglamento General de Protección de Datos + LOPDGDD + LO 7/2021 + LOPJ + Ley 50/1981

02. Las autoridades de control de protección de datos (III)

BRECHAS DE SEGURIDAD	INTERVINIENTES

• Ataques
• Vulnerabilidad de página web
• Envíos de correos electrónicos sin copia oculta
• Envío erróneo de información a terceros
• Documentos en la basura
• Robo
• Pérdidas de USB con datos personales
 	
• **Formas de identificación:**
  • Interna
  • Externa
	• Responsable del tratamiento
	• Encargado del tratamiento
	• Delegado de Protección de Datos
	• Afectados (“interesados”)
	• Trabajadores
	• Redes sociales/Medios de comunicación
	• Autoridades de Protección de Datos

02. Las autoridades de control de protección de datos (IV)



¿Quién sería la Autoridad de Protección de Datos competente?

02. Las autoridades de control de protección de datos (V)

ÍNDICE

ÍNDICE

– No estamos arrancando: YA estamos en marcha. Y seguimos

– Tener una Política de Seguridad de la Información está bien. Dejarla sin tocar, y acomodarse, es garantía de fracaso.

– Estamos:
  - Dotando al subcomité de una oficina de seguridad
  - Dotando al subcomité de las funciones de SOC que le pide la PSI

- Oficina de seguridad
  - En proceso la elaboración del perfil de cumplimiento para simplificar el proceso de adecuación de los sistemas de información. Criterios comunes en:
    - Categorización de los sistemas
    - Análisis de riesgos
    - Cumplimiento y certificación
  - Diseño de las propuestas de mejora derivadas del cuestionario de Madurez (del CCN)
- SOC
  - Capacidades de auditoría técnica de los sistemas de información
  - Coordinación en la gestión de ciberincidentes severos

Fondos UE exclusivos para ciberseguridad en los sistemas de Justicia:
2 Millones para cada CC.AA.

Requiere unos **requisitos mínimos de seguridad** (ficha adjunta)

*Las CCAA están **desarrollando proyectos** para cumplir con los **requisitos mínimos** y si ya los tienen superados deben abordar proyectos que eleven el nivel de de seguridad aún más.*

Gracias por su atención

GOBIERNO DE ESPAÑA

MINISTERIO DE JUSTICIA

SECRETARÍA DE ESTADO DE JUSTICIA

SECRETARÍA GENERAL PARA LA INNOVACIÓN Y CALIDAD DEL SERVICIO PÚBLICO DE JUSTICIA

AGENDA 2030