

Una administración abierta empieza por su modelo de trabajo

Miguel Carrero

**Vice President, Security Service Providers
& Strategic Accounts**

Construcción de un Gobierno Abierto

“Iniciativa cuyo objetivo es que los ciudadanos colaboren en la creación y la mejora de los servicios públicos”

Construcción de un Gobierno Abierto

“Iniciativa cuyo objetivo es que los ciudadanos colaboren en la creación y la mejora de los servicios públicos”



Construcción de un Gobierno Abierto

“Iniciativa cuyo objetivo es que los ciudadanos colaboren en la creación y la mejora de los servicios públicos”



Jerarquía de las necesidades humanas

SEGÚN LA PIRÁMIDE DE MASLOW

20 minutos



Construcción de un Gobierno Abierto

“Iniciativa cuyo objetivo es que los ciudadanos colaboren en la creación y la mejora de los servicios públicos”



Jerarquía de las necesidades humanas

SEGÚN LA PIRÁMIDE DE MASLOW

20 minutos



“No hay Gobierno abierto sin un Gobierno seguro”

Construcción de un Gobierno Seguro

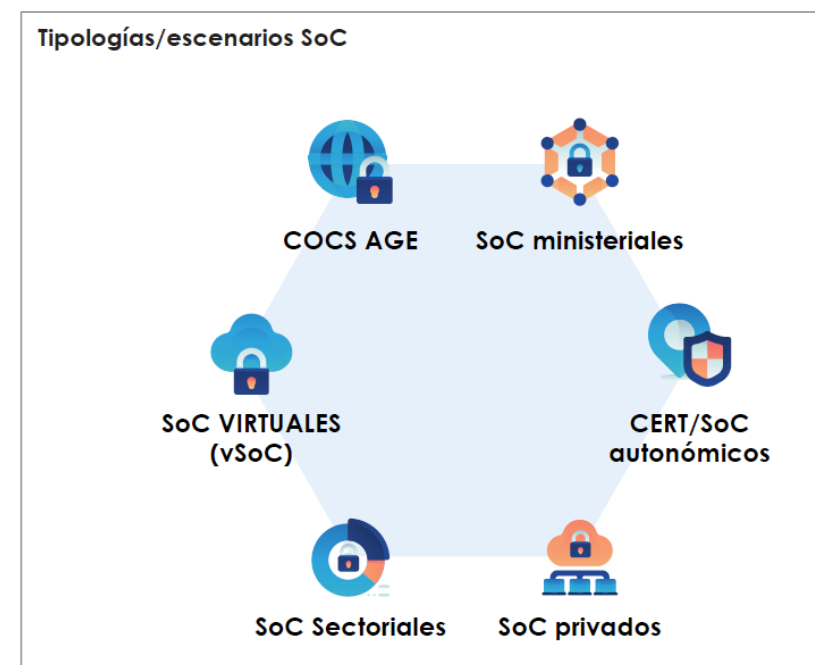
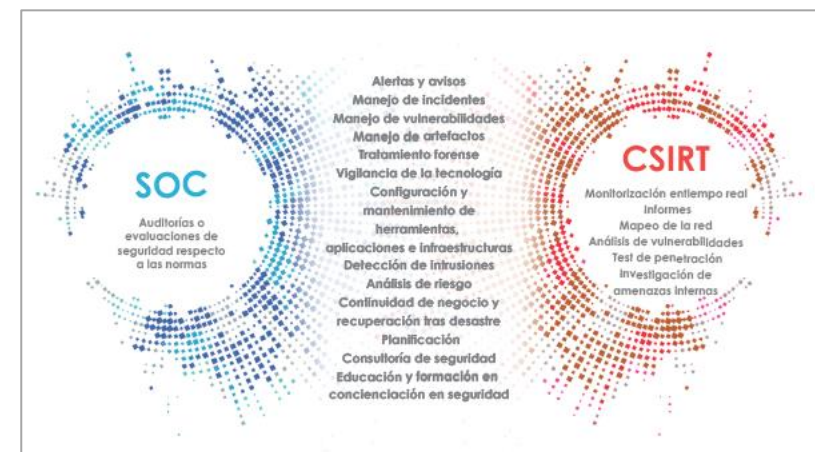
- Importancia del Esquema Nacional de Seguridad (ENS) que ofrece un planteamiento común de principios básicos, requisitos mínimos y medidas de seguridad.
- Proceder dentro del marco de actuación del ENS



Construcción de un Gobierno Seguro

Pilares básicos:

- Racionalización y efectividad de la seguridad
- Consistencia e Interoperabilidad que permite niveles de especialización y compartición
- Seguridad que se consume como servicio



Construcción de un Gobierno Seguro en el entorno actual

Caso éxito Consellería de Sanidad Universal y Salud Pública Generalitat Valenciana

- Conselleria de Salud de la Generalitat Valenciana confió en WatchGuard-Cytomic la seguridad de su entorno de teletrabajo



- **Desafío**
 - Gestión de un entorno heterogéneo y disperso por la llegada de la pandemia.
 - Preparación a contrarreloj de la plantilla para adoptar el teletrabajo, y organizar una gestión centralizada y coordinada de las conexiones con la premisa de la seguridad.
 - Securización de 2.600 equipos particulares de sus trabajadores.

Construcción de un Gobierno Seguro en el entorno actual

Caso éxito Consellería de Sanidad Universal y Salud Pública Generalitat Valenciana

- Conselleria de Salud de la Generalitat Valenciana confió en WatchGuard-Cytomic la seguridad de su entorno de teletrabajo



Antonio Grimaltos Vidal

Oficina de seguridad de la Información.
Consellería de Sanidad Universal y
Salud Pública | Generalitat Valenciana

- **Desafío**

- Gestión de un entorno heterogéneo y disperso por la llegada de la pandemia.
- Preparación a contrarreloj de la plantilla para adoptar el teletrabajo, y organizar una gestión centralizada y coordinada de las conexiones con la premisa de la seguridad.
- Securización de 2.600 equipos particulares de sus trabajadores.

Caso éxito Consellería de Sanidad Universal y Salud Pública Generalitat Valenciana



La hora más oscura

6 de marzo de 2020



USO OFICIAL



CCN-CERT – Medidas de seguridad para el acceso remoto

Abstract: Garantizar la seguridad de los sistemas de información involucrados en los accesos remotos por si se activan medias de contención o de teletrabajo excepcionales. En la actualidad existen múltiples campañas de *ransmoware* activas y dado que las conexiones remotas pueden ser una vía de entrada de malware o personas no identificadas a los sistemas, se desarrolla en este documento una breve explicación de medias complementarias a cada organismo en sus accesos remotos.

#XIVJORNADASCNCERT

Caso éxito Consellería de Sanidad Universal y Salud Pública Generalitat Valenciana



La hora más oscura

6 de marzo de 2020



CCN-C

Abstract: Garantiz
por si se activan m
campañas de rans
malware o person
explicación de med

#XIVJORNADASCNCERT



La hora más oscura

6 de marzo de 2020

3.2 Equipos portátiles corporativos

Debe considerarse la primera forma de acceso, al contemplar las medidas de seguridad del organismo. Aunque deben cumplir las siguientes medidas:

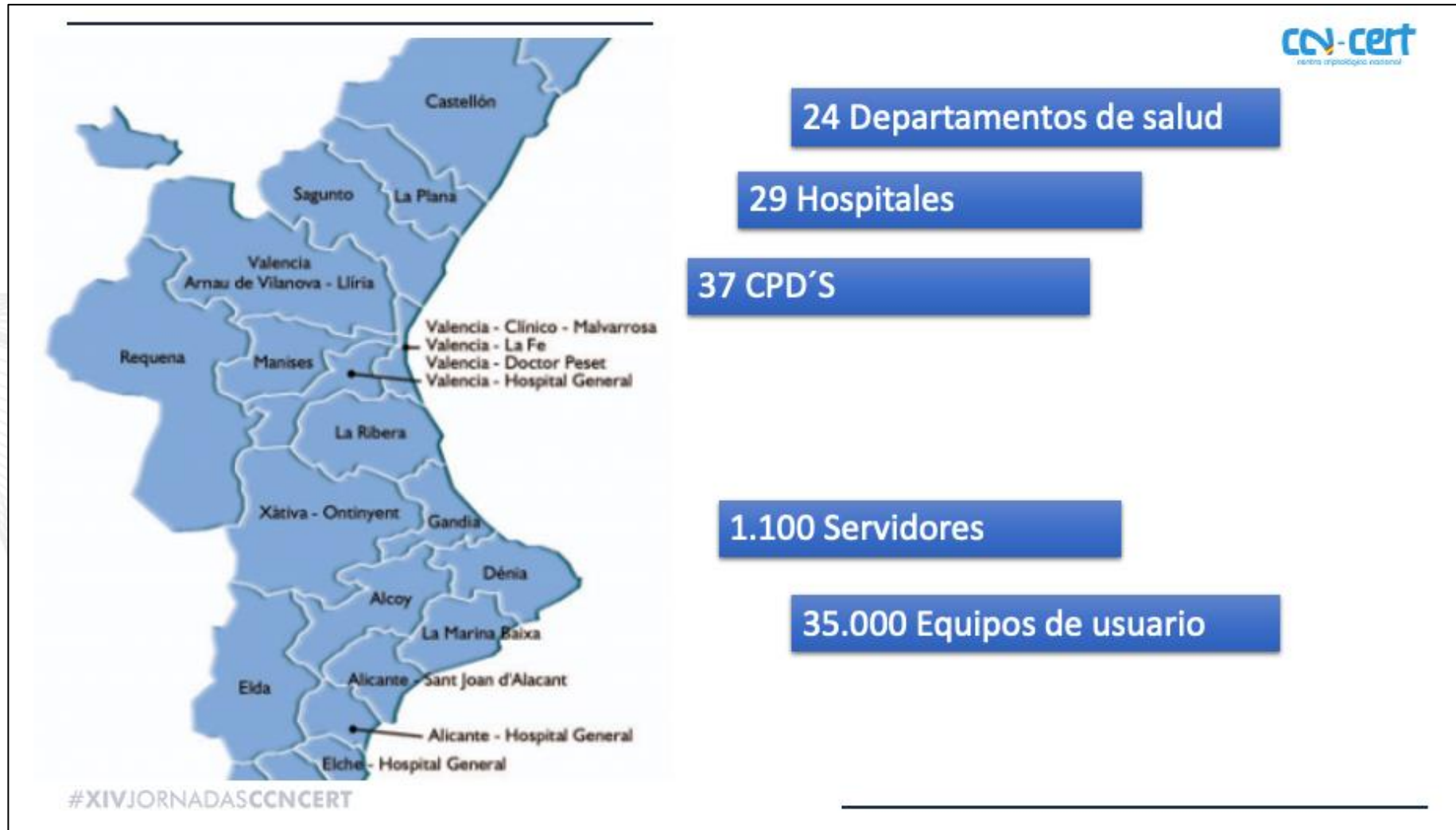
- Tener las últimas actualizaciones de sistemas operativo instalada
- Aplicaciones ofimáticas, lectores de pdf y de uso cotidiano, actualizadas a la última versión de parches de seguridad
- Tener antivirus instalado
- Estado del antivirus actualizado como sugerencia al día de conectar, en caso de no poderse al menos tres (3) días antes.
- Se sugiere tener Endpoint instalado.

3.3 Equipos personales

Estos pueden ser los equipos más vulnerables. Por ello, es la última opción de conectividad. Dado el caso de su utilización, se deben aplicar las medidas anteriores y además ponerlo en conocimientos de los equipos de seguridad del organismo por si se deben establecer medidas adicionales a las establecidas.

#XIVJORNADASCNCERT

Caso éxito Consellería de Sanidad Universal y Salud Pública Generalitat Valenciana



Caso éxito Consellería de Sanidad Universal y Salud Pública Generalitat Valenciana



Caso éxito Consellería de Sanidad Universal y Salud Pública Generalitat Valenciana

• Solución

- WatchGuard Advanced EPDR cumplía con todos los criterios fijados por la Conselleria de Salud y cuenta con ENS Alto
- La solución superó todas las pruebas realizadas por el Equipo de Respuesta ante Incidentes de Seguridad (CSIRT).
- Permitía la supervisión continua y centralizada de todos los equipos, la detección y clasificación de toda la actividad, y el bloqueo de los comportamientos anómalos de usuarios, máquinas y procesos.



La hora más oscura

13 de marzo de 2020

- CONTROL CENTRALIZADO
- PERMITE CONFIGURAR LA **PRIVACIDAD**
 - No guardamos datos del usuario solo la ip (de su router) y el nombre del equipo.
- UTILIDADES DE LA CONSOLA PARA CONFIGURAR DIFERENTES GRUPOS
- UTILIDADES DE LA CONSOLA PARA INVESTIGAR INCIDENTES
- POSIBILIDAD DESDE LA CONSOLA DE AISLAR EN EQUIPOS Y SOLO DEJARLE CONEXIÓN A LOS SERVIDORES DE PANDA
- POSIBILIDAD DE LIMITAR LAS PÁGINAS A LAS QUE SE ACCEDE.
- POSIBILIDAD DE CONTROLAR EL SOFTWARE INSTALADO.
 - Importantísimo a la hora de la desescalada (solo se autorizaba la desinstalación si se ha desinstalado el software de VPN)



- FÁCIL DE DESPLEGAR
- NO RALENTIZA LOS EQUIPOS
- WINDOWS, MAC Y LINUX

Certificada para el
ENS Nivel ALTO

#XIVJORNADASCCNCERT

Caso éxito Consellería de Sanidad Universal y Salud Pública Generalitat Valenciana

• Resultado

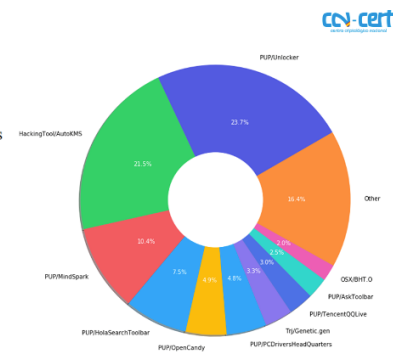
- La Consellería permitió mantener operativos a sus empleados en los peores momentos protegiendo la información y los sistemas corporativos continuamente.
- Habilita las conexiones remotas en la actualidad.
- Se recibieron entre 50.000 y 70.000 alertas de ciberseguridad, 1.464 correspondían a distintos tipos de malware. Todos los ataques fueron detectados y neutralizados por la solución.
- El organismo ha logrado implantar una cultura de ciberseguridad que muchos usuarios no tenían.
- La Consellería de Salud está desplegando la plataforma WatchGuard Orion de detección, búsqueda, investigación y respuesta de múltiples usuarios, diseñada para los equipos de operaciones de seguridad.

La hora más oscura

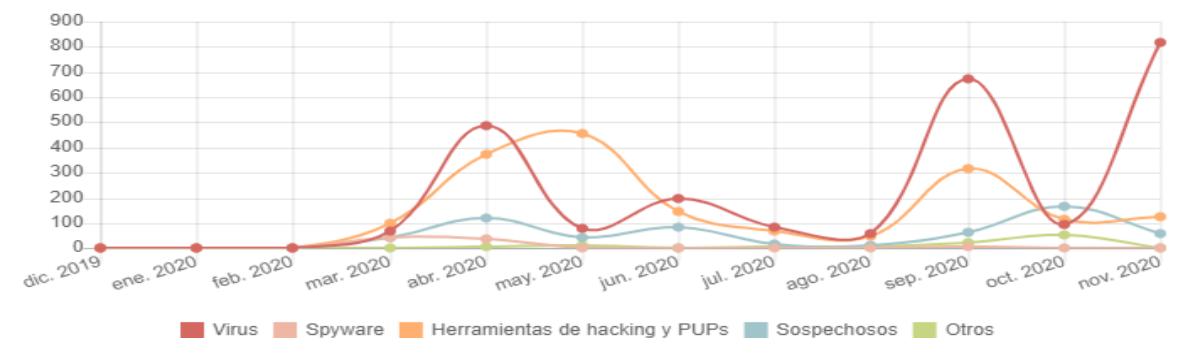
1.997 máquinas registradas y comunicantes

1.464 detecciones de Malware únicas respuestas

23,39 % máquinas afectadas con detecciones de Malware



AMENAZAS DETECTADAS



Caso éxito Consellería de Sanidad Universal y Salud Pública Generalitat Valenciana



Valencia, 12 de mayo de 2022

Estimados Sres. D. Juan Miguel Signes y D. Antonio Grimaltos,

nos ponemos en contacto con ustedes para informarles del fallo del comité de premiados de ISACA Valencia 2022.

Se entrega el **Premio de Seguridad de los Sistemas de Información 2022** a la **Conselleria de Sanitat**, "la organización autonómica que más se ha comprometido con el tratamiento de la pandemia, no solo a nivel sanitario, sino a nivel de seguridad".

La CdS ha demostrado una gran capacidad de prevención, anticipándose al teletrabajo, desplegando soluciones de endpoint en los puestos remotos días antes de la declaración del estado de alarma, actualmente con la plataforma **EMMA-VAR** de control de acceso remoto y cumplimiento del **ENS**, y una capacidad de respuesta a incidentes gestionando todo tipo de amenazas durante este tiempo, y una capacidad evolutiva de la seguridad disponiendo un piloto de autodescubrimiento y gestión de la ciberseguridad interna para intercambio seguro entre médicos, pacientes, y centros de educación para comunicación de datos sensibles. A lo largo de estos últimos años, ha demostrado una gran capacidad y compromiso con la seguridad, siendo un ejemplo para otras instituciones.

El premio será entregado la mañana del Viernes 20 de Mayo durante la sesión del XIV Congreso de ISACA Valencia. Asimismo, están invitados al almuerzo de trabajo que se realizará tras la sesión del Congreso.

Enhorabuena de parte del Comité de Premios 2022 y de la Directiva de ISACA Valencia. ¡Esperamos encontrarnos!

Atentamente,



Alejandro Aracil Vicedo
Presidente de ISACA Valencia

ISACA VALENCIA
ASOCIACIÓN DE AUDITORÍA, SEGURIDAD Y GOBIERNO DE LOS SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN DE LA CV
Asociación sin ánimo de lucro inscrita en el Registro de Asociaciones de Valencia, Sección 1ª. N° CV-01-036991-V CIF G-97625156

www.isacavalencia.org

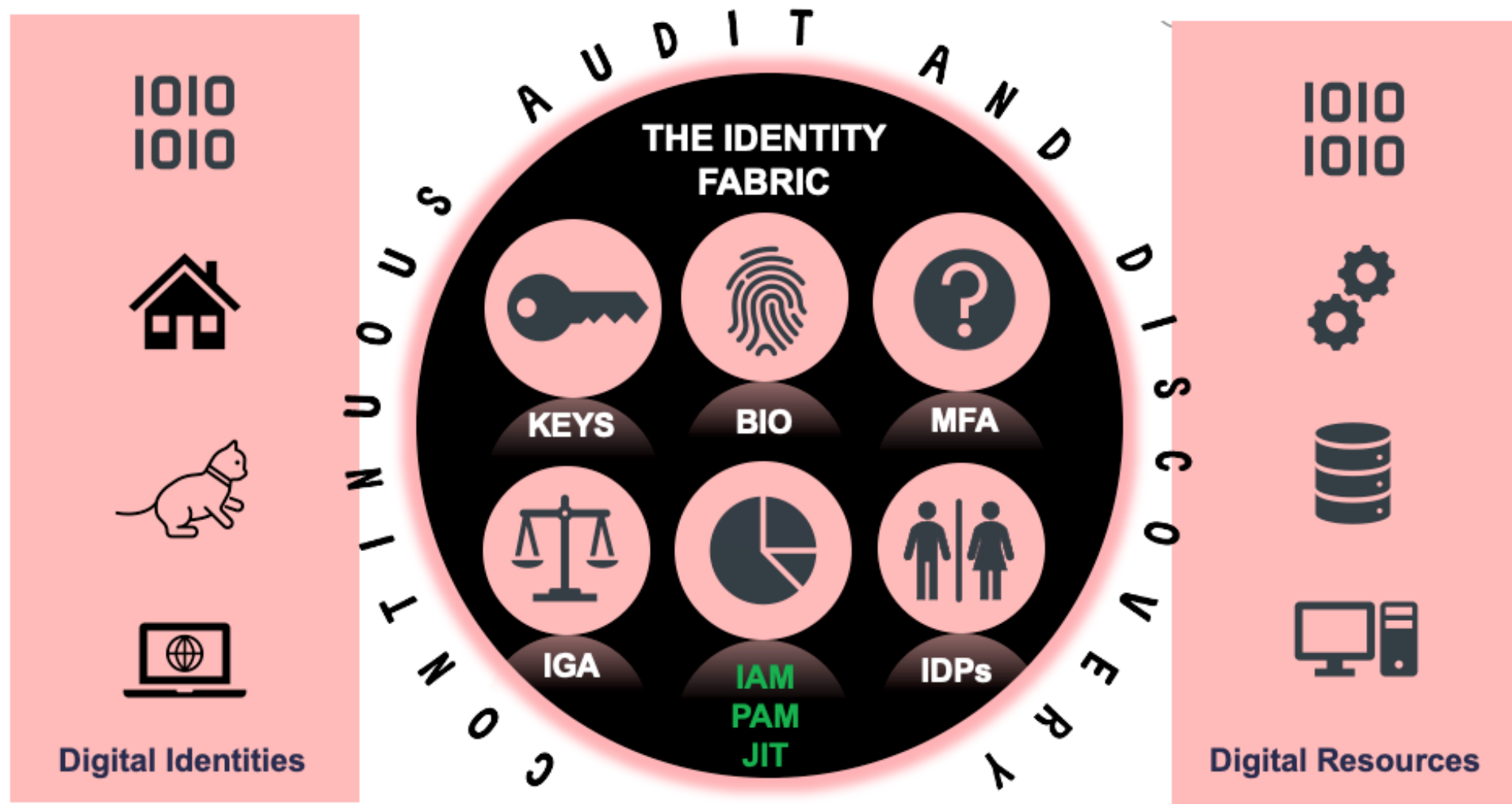
ISACA Valencia 2022

Premio de Seguridad de los Sistemas de Información 2022 a la Conselleria de Sanitat.

Construcción de un Gobierno Abierto



Construcción de un Gobierno Abierto



Source: KuppingerCole

Gracias!

¿Hablamos?

Strategic.accounts@watchguard.com