Hacia un marco de gobierno de la seguridad para ciudades inteligentes

David G.ROSADO
Grupo de Investigación GSyA
Universidad de Castilla-La Mancha
David.GRosado@uclm.es

Luis Enrique SÁNCHEZ
Grupo de Investigación GSyA
Universidad de Castilla-La Mancha
Luise.Sanchez@uclm.es

Ferney MARTÍNEZ
Grupo de Investigación GSyA-PRODIN
Universidad de Castilla-La Mancha
Ferney.Martinez@alu.uclm.es

Carlos BLANCO
Grupo de Investigación GSyA
Universidad de Cantabria
Carlos.blanco@unican.es

Manuel A. SERRANO
Grupo de Investigación Alarcos
Universidad de Castilla-La Mancha
Manuel.Serrano@uclm.es

Eduardo FERNÁNDEZ-MEDINA
Grupo de Investigación GSyA
Universidad de Castilla-La Mancha
Eduardo.Fdezmedina@uclm.es

Resumen - **Las ciudades inteligentes son cada vez más populares. La posibilidad de utilizar los avances tecnológicos para ofrecer mejores servicios a los ciudadanos, o mejores funciones gubernamentales, resulta muy atractiva. Sin embargo, las ciudades inteligentes también implican riesgos de seguridad, ya que existen muchos problemas de ciberseguridad, vulnerabilidades y tipos de ciberataques que pueden afectar a las ciudades inteligentes. Una forma de reducir estos problemas de seguridad es mediante la creación de un marco de gobierno de la seguridad específico para las ciudades inteligentes. Este es nuestro principal objetivo. Se trata de una tarea muy complicada, y de hecho todo un reto, debido a las características distintivas de las Smart cities. Por ello, como aproximación inicial a la creación de un marco completo de gobierno de la seguridad para Smart cities, hemos considerado la estructura de dominios y procesos propuesta por COBIT. Esta estructura se ha modificado con el fin de abordar las características de las Smart cities y los problemas de seguridad relacionados con ellas.**

***Terminos*- Ciudades Inteligentes, Seguridad, Gobernanza**

I. Introducción

Una ciudad puede considerarse como un sistema de sistemas con una historia única y establecido en un contexto ambiental y social específico. Una ciudad puede considerarse "inteligente" cuando tiene la capacidad de combinar eficazmente todos sus recursos y alcanzar las metas y propósitos que previamente se ha planteado [1]. Una ciudad inteligente es un nombre que inspira una visión de una ciudad donde los componentes clave de infraestructura y servicios se integran de tal manera que las características y aplicaciones se pueden combinar fácilmente con cualquier capacidad que existiera antes [2]. Las nuevas tecnologías, junto con una conectividad más rápida y sencilla, permiten a las ciudades optimizar recursos, ahorrar dinero y, al mismo tiempo, brindar mejores servicios a sus ciudadanos [3]. Por lo tanto, las ciudades inteligentes podrían proporcionar [4]: servicios mejores y más cómodos para los ciudadanos; mejor gobernanza de la ciudad; un mejor entorno de vida; una industria más moderna, y una economía dinámica e innovadora.

Se espera que el mercado mundial de ciudades inteligentes crezca a una tasa de crecimiento anual compuesta del 25,8% entre 2023 y 2030 hasta alcanzar los 3.728,3 mil millones de dólares en 2030 [5], con la mitad de ciudades inteligentes de América del Norte y Europa. Los servicios electrónicos para los ciudadanos, como los pagos electrónicos, el intercambio electrónico, etc., brindarán a los ciudadanos acceso en tiempo real a datos personales y servicios relacionados.

Para el ciudadano, los beneficios de esta integración de los sistemas de la ciudad incluyen servicios personalizados, acceso a la información, mayor transparencia en los procesos de toma de decisiones del sector público y apoyo para ayudarse mutuamente de manera más efectiva. Para los líderes empresariales locales, los beneficios incluyen una gestión más eficiente y nuevas oportunidades comerciales. Para los proveedores de servicios, los beneficios incluyen mayores sinergias, ofertas de servicios individualizados y nuevas formas de satisfacer las necesidades de los clientes [6].

La ciberseguridad en el contexto de las ciudades inteligentes es un tema controvertido. Nuestra infraestructura urbana está ahora bajo la amenaza constante de ataques cibernéticos y una gama cada vez mayor de desastres, tanto naturales como provocados por el hombre [7]. La ciberseguridad debe abordar no sólo los ataques deliberados, como los de empleados descontentos, el espionaje industrial y los terroristas, sino también los compromisos inadvertidos de la infraestructura de información debido a errores de los usuarios, fallas de equipos y desastres naturales [8]. En un entorno de ciudad inteligente, los servicios deficientes podrían causar daños a gran escala e incluso afectar la estabilidad y la seguridad nacionales. Una ciudad inteligente requiere nuevos niveles de confidencialidad, integridad, disponibilidad, defensa y privacidad [9].

Dado que los ciudadanos digitales están cada vez más equipados con los datos disponibles sobre su ubicación y actividades, la privacidad parece desaparecer [10]. La información del área del hogar recopilada y administrada por aplicaciones domésticas inteligentes puede allanar el camino para revelar el estilo de vida altamente sensible a la privacidad de las residencias e incluso causar pérdidas económicas [11].

Estos problemas de seguridad se pueden abordar desde la perspectiva de tener múltiples políticas y controles de seguridad no relacionados entre sí. Esta puede ser una opción aceptable para sistemas más simples, pero las ciudades inteligentes son más complejas e integran sistemas muy diferentes. Una solución a este problema puede ser la creación de un marco de gobierno de la seguridad para las ciudades inteligentes. Un marco de gobierno de TI se puede definir como la especificación del marco de derechos de decisión y responsabilidad para fomentar el comportamiento deseable en el ámbito de TI [12].

Nuestro principal objetivo es desarrollar un marco de seguridad de gobierno para ciudades inteligentes. Esta

investigación debe considerar cómo evolucionan las tecnologías y conceptos relacionados con las ciudades inteligentes mientras las propias ciudades inteligentes continúan su implementación. Esta serie de características implican que sea muy complicado crear el framework desde cero sin tener primero unos fundamentos adecuados que establezcan un punto base para crear el framework.

Por tanto, el objetivo de este artículo expondrá nuestra aproximación inicial a la creación de una propuesta marco para el gobierno de la seguridad en entornos de ciudades inteligentes. Este marco tiene como principal objetivo facilitar la relación entre los objetivos estratégicos de seguridad y la gestión de la ciudad inteligente. Para la creación de esta propuesta de marco de gobierno, basamos nuestra investigación en los dominios y procesos definidos por el marco general de gobierno de TI, COBIT. Con la ayuda de las indicaciones dadas en esta norma y considerando las características específicas de seguridad y privacidad de una ciudad inteligente, se ha definido el marco SGSC (Gobierno de Seguridad en Ciudades Inteligentes).

Este artículo tiene la siguiente estructura: en primer lugar, se abordará una introducción a los diferentes temas necesarios para entender nuestro framework, por ejemplo COBIT, o las vulnerabilidades específicas de una ciudad inteligente. Posteriormente, se expondrá nuestra propuesta de gobierno de la seguridad definiendo los diferentes dominios y procesos que la componen. Finalmente, se comenta un apartado con las conclusiones y trabajos futuros.

II. TRABAJO RELACIONADO

En esta sección se explicarán los diferentes temas relacionados con nuestro framework. Primero, describiremos la propuesta COBIT para garantizar la gobernanza adecuada de TI. En consecuencia, definiremos cómo se puede abordar la ciberseguridad para asegurar una ciudad inteligente y además, en este apartado se describirán las principales vulnerabilidades y ciberataques que puede sufrir una ciudad inteligente. Finalmente, explicaremos los diferentes dominios que generalmente se pueden identificar en una ciudad inteligente, y esta clasificación, junto con las vulnerabilidades y ciberataques explicados anteriormente, nos permitirá abordar adecuadamente la definición de controles de seguridad específicos para las ciudades Inteligentes.

A. COBIT:

COBIT [13] es un marco de gobernanza de las tecnologías de la información que proporciona una serie de buenas prácticas y actividades para la gestión que tiene como objetivo alinear los requisitos de control con las cuestiones técnicas y riesgos de negocio, lo que permite incrementar el valor de las organizaciones a través de la tecnología. Se pretende que COBIT sea posible de aplicar a cualquier organización, independientemente de su tamaño. Para integrar la seguridad al modelo COBIT se toma como base el modelo utilizado por BMIS (Business Model for Information Security) pero incorporando la visión holística de COBIT y sus componentes, presentando así un enfoque más orientado al negocio para la gestión de la seguridad de la información.

COBIT proporciona un lenguaje común para referirse a la protección de la información, cambiando la visión tradicional de la inversión adicional en seguridad de la información. Para lograr estos objetivos, COBIT define un marco que clasifica los procesos de las unidades de TI de las organizaciones en cinco dominios principales: i) Evaluar, dirigir y monitorear (EDM); ii) Alinear, planificar y organizar (APO); iii) Construir, adquirir e implementar (BAI); iv) Entrega, servicio y soporte (DSS); y v) Monitorear, evaluar y valorar (MEA).

COBIT es, por tanto, un marco de gobierno de alto nivel destinado a ser aplicable a cualquier tipo de organización en cualquier escenario. Esta característica que puede considerarse positiva es, en cambio, una propiedad negativa porque al ser un marco tan genérico complica su adopción por parte de las empresas. En nuestro caso, usaremos la forma en que COBIT define y organiza sus diferentes dominios y procesos para construir nuestro marco SGSC.

B. Ciberseguridad en Smart City

Cuando las ciudades se vuelven más inteligentes, las personas pueden sufrir una serie de amenazas a la seguridad y la privacidad debido a las vulnerabilidades de las aplicaciones de las ciudades inteligentes [14]. Por ejemplo, los atacantes maliciosos podrían lanzar ataques de denegación de servicio, interrumpiendo la detección, la transmisión y el control para degradar la calidad de los servicios inteligentes en una ciudad inteligente [15].

Es difícil ignorar la cuestión de la ciberseguridad en referencia a la creciente presencia y uso de dispositivos inteligentes en el hogar y el lugar de trabajo en todo el mundo. Son convenientemente más inteligentes, más livianos, portátiles y con excelentes capacidades de almacenamiento y conectividad [16]. Los hechos que se toman en consideración para identificar los problemas de seguridad de la información en una ciudad inteligente incluyen factores de gobernanza, factores sociales/económicos y, lo más importante, factores tecnológicos [17].

Las soluciones de ciudades inteligentes utilizan conjuntos complejos y en red de tecnologías digitales e infraestructura de TIC para gestionar diversos sistemas y servicios de la ciudad. Cualquier dispositivo que dependa de software para funcionar es vulnerable a ser pirateado [18]. Si uno o más servicios dependientes de la tecnología no funcionan, probablemente causará mucho caos en cualquier ciudad, por ejemplo, sistemas de control de tráfico, falta de transporte público, un suministro inadecuado de electricidad o agua, calles oscuras o la interrupción del servicio. recolección de basura. Es posible que ese escenario no sea tan improbable como cree.

Vulnerabilidades

Las vulnerabilidades en una ciudad inteligente podrían permitir que un atacante penetre en una red, obtenga acceso para controlar el software y altere las condiciones de carga para desestabilizar el sistema de maneras impredecibles [19]. La vulnerabilidad de los sistemas se ve exacerbada por una serie de cuestiones o problemas que incluyen [20]: i) Seguridad y cifrado débiles; ii) el uso de sistemas heredados inseguros y un mantenimiento deficiente; iii) Grandes y complejas superficies de ataque e interdependencias; iv) Efectos en cascada; v) Falta de pruebas de seguridad cibernética; vi) Falta de equipos de respuesta a emergencias informáticas; vii) Problemas de implementación de parches; viii) Errores simples con gran impacto; ix) Falta de planes de emergencia ante ciberataques; x) Susceptibilidad a la denegación del servicio.

Ataques ciberneticos

Los ciberataques pueden ser realizados por naciones hostiles, grupos terroristas, ciberdelincuentes, colectivos de piratas informáticos y piratas informáticos individuales. En [21] se

definen tres formas de ciberataque: ataques de disponibilidad que buscan cerrar un sistema o negar el uso del servicio; ataques a la confidencialidad que buscan extraer información y monitorear la actividad; y ataques a la integridad que buscan ingresar a un sistema para alterar información y configuraciones. Además de estos tres, en [22] los autores definen dos categorías más a tener en cuenta que son autenticidad y no repudio/responsabilidad.

A través de las nuevas tecnologías desplegadas para una ciudad inteligente, la ciudad permite disponer de un conjunto de servicios urbanos que se vuelven más inteligentes [23]. Todas las formas de tecnologías de ciudades inteligentes son vulnerables a los ciberataques. Hay una serie de puntos débiles, incluidos los sistemas SCADA, los sensores y microcontroladores del Internet de las cosas, y las redes de comunicación y los conmutadores de telecomunicaciones [24, 25]. Esto podría tener un gran impacto dependiendo de cómo los sistemas afectados utilicen los datos e interactúen con otros sistemas [26].

Las ciudades están llenas de una gran cantidad de cámaras CCTV cuya seguridad es muy variable. Al atacar las comunicaciones o los sistemas informáticos centrales, un actor malintencionado podría atacar los propios dispositivos de señalización de tráfico, provocando interrupciones locales y regionales que aumenten la congestión y disminuyan la seguridad en áreas objetivo específicas [27]. La gestión del tráfico podría verse perjudicada al piratear el sistema de navegación que dirige al conductor del autobús a la ciudad por una ruta equivocada, debido a la información falsa sobre el volumen del tráfico [28].

En caso de accidente de tráfico, una intrusión maliciosa que comprometa la comunicación entre los primeros auxilios y los centros operativos podría impedir su correcta localización y el envío más eficiente de las unidades de emergencia [29, 30].

C. *Dominios en Smart City*

Una ciudad inteligente se puede definir como un área urbanizada donde múltiples sectores cooperan para lograr resultados sostenibles a través del análisis de información contextual en tiempo real compartida entre sistemas de tecnología operativa y de información específicos del sector [31]. El proceso de transformación de una ciudad en una ciudad inteligente involucra seis áreas diferentes de actividad, como Economía, Medio Ambiente, Movilidad, Gobierno, Personas y Vida (Vivienda y fuera de lo común). Para cada una de estas áreas existen diferentes enfoques [31-33] donde se definen un conjunto de dominios para la ciudad inteligente.

Muchos de estos dominios pueden integrarse en otros debido a la similitud entre sectores para la ciudad o para los ciudadanos, por lo que hemos considerado este conjunto de dominios más apropiados para una ciudad inteligente relacionados con las principales áreas de actividad, como se muestra en la Tabla I.

Tabla I:
ÁREAS DE ACTIVIDAD Y DOMINIOS EN UNA SMART CITY

Áreas de actividad	Dominios
Economía	Economía
Ambiente	Medio ambiente, Gestión energética, Residuos
Movilidad	Servicios de Movilidad, Seguridad y Emergencias
Gobierno	Gobierno, Servicios Sociales
Gente	Edificaciones, Telecomunicaciones y Medios Comunicación
Viviendo	Educación, Salud, Hogares

Estos dominios, junto con los dominios y procesos de COBIT, se utilizarán para crear el marco SGSC.

III. Framework SGSC

Nuestra propuesta de marco de gobierno denominada SGSC (Security Governance in Smart Cities) pretende abarcar el gobierno de la seguridad en las Smart Cities a lo largo de todo su ciclo de vida. Para crear el marco SGSC, hemos considerado la estructura de dominios de procesos y procesos propuestos por COBIT. Esa estructura se ha utilizado como base para crear el esqueleto del marco SGSC.

Así, la estructura básica de cuatro dominios de proceso identificados por COBIT se modificó para satisfacer las necesidades específicas de las ciudades inteligentes. Además de las modificaciones en estos dominios de proceso, se ha añadido un quinto dominio que tiene como finalidad analizar las amenazas a la seguridad de las ciudades Inteligentes. Como resultado, el marco SGSC se compone de seis dominios diferentes. La Figura 1 muestra una comparación entre los dominios de proceso de COBIT y el marco SGSC.

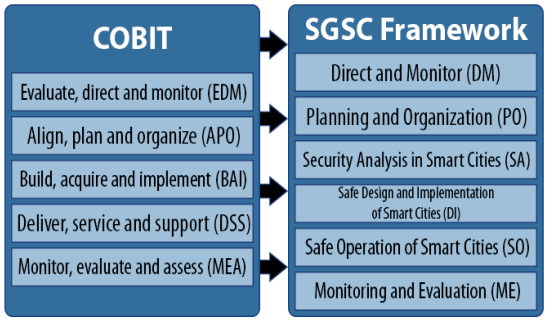

Fig 1. Comparación entre los dominios de proceso de COBIT y SGSC

En las siguientes subsecciones se explicarán los seis dominios que forman el Marco SGSC y los diferentes procesos contenidos en ellos.

A. *Dirección y Supervisión (DM)*

El principal objetivo de este dominio es garantizar que los objetivos empresariales se alcancen mediante la evaluación de las necesidades, condiciones y opciones de las partes interesadas. Finalmente, este dominio tiene como objetivo monitorear el desempeño, el cumplimiento y el progreso con respecto a los objetivos estratégicos. Este dominio está formado por 14 procesos diferentes explicados en la Tabla II.

Tabla II:
PROCESOS DE DOMINIO DIRECCIÓN Y SUPERVISIÓN (DM)

Id	Proceso	Objetivo
DM1	Garantizar el establecimiento y mantenimiento.	Asegurar que las decisiones relacionadas con TI se tomen en línea con las estrategias y objetivos.
DM2	Garantizar la entrega de beneficios	Para asegurar un valor óptimo de las iniciativas, servicios y activos de TI.
DM3	Garantizar la optimización del riesgo	Garantizar que los riesgos de la de TI no excedan los límites.
DM4	Garantizar la optimización de recursos	Garantizar que las necesidades de recursos se cubran.
DM5	Garantizar la transparencia de las partes.	Garantizar que la comunicación a los grupos de interés sea efectiva.

B. *Planificar y Organizar (PO)*

El dominio de Planificación y Organización cubre la estrategia y tácticas relacionadas con la ciudad en general. El objetivo principal de este dominio es identificar cómo la implementación de los diferentes sistemas que constituyen una ciudad inteligente puede contribuir a alcanzar los objetivos específicos de la ciudad.

En este caso se mantiene tanto el nombre como la finalidad

del dominio respecto a COBIT, pero hay cambios en cuanto a los procesos que lo forman ya que será necesario implementar un plan de seguridad específico para las ciudades Inteligentes. Este dominio está formado por 14 procesos diferentes explicados en la Tabla III.

Tabla III:
PROCESOS DE PLANIFICACIÓN Y ORGANIZACIÓN (PO)

Id	Proceso	Objetivo
PO1	Definir el plan estratégico de seguridad.	Mejor equilibrio entre las diferentes oportunidades que brinda la TI.
PO2	Definir la arquitectura de la información.	Satisfacer los requerimientos de la organización.
PO3	Definir la dirección tecnológica	Utilizar todas las posibilidades que ofrecen las tecnologías.
PO4	Definir los procesos y relaciones de seguridad.	Servicios informáticos seguros con definición de responsabilidades.
PO5	Gestionar la inversión en seguridad	Satisfacer necesidades de seguridad gestionando la financiación.
PO6	Comunicar los objetivos generales a la Dir. Tecnológica.	Asegurar el conocimiento y comprensión de los usuarios sobre los objetivos generales de la ciudad.
PO7	Gestionar los recursos humanos de seguridad.	Maximizar la contribución del personal de seguridad usando técnicas de gestión de RRHH.
PO8	Gestión de riesgos de seguridad	Garantizar la consecución de los objetivos de seguridad frente a las amenazas relacionadas.
PO9	Desarrollar políticas para un plan de seguridad.	Transformar políticas de gobernanza en políticas de seguridad.
PO10	Identificar responsables del plan de seguridad.	Identificar los roles que gestionarán el plan de seguridad.
PO11	Definir los objetivos y alcance del plan de seguridad.	Definir los objetivos concretos y el alcance del plan de seguridad.
PO12	Garantizar la alineación entre los objetivos y el plan de seguridad.	La estrategia de ciudad adoptada está alineada con el plan de seguridad previamente definido.
PO13	Medir la eficiencia del plan de seguridad	Definir métricas (KPIs) para el plan de seguridad.
PO14	Creación del marco legal sobre la ciudad inteligente	Creación de un marco legal que para los nuevos escenarios legales.

C. Análisis de Seguridad en Ciudades Inteligentes (SA)

El dominio de Análisis de Seguridad en Ciudades Inteligentes tiene el objetivo principal de abordar los problemas específicos de seguridad en las ciudades Inteligentes. Este dominio es una novedad con respecto a COBIT, la inclusión en el marco se debe al hecho de que COBIT es un marco más general y no se centra especialmente en la seguridad, lo cual es contrario a nuestro objetivo. Así, en este dominio se ha creado un conjunto de procesos diferentes, no considerados por COBIT.

Estos procesos están enfocados a analizar las diferentes propiedades de seguridad que pueden afectar a la ciudad inteligente. Estas propiedades de seguridad dependen de los requisitos, el modelo y el alcance de la ciudad inteligente. También cubre el análisis de los riesgos específicos de un proyecto de ciudad inteligente. Este dominio está formado por 5 procesos diferentes explicados en la Tabla IV.

Tabla IV:
PROCESOS DE ANÁLISIS DE SEGURIDAD (SA)

Id	Proceso	Objetivo
SA1	Definir los requisitos de seguridad.	Definir los diferentes requisitos de seguridad.
SA2	Identificar alternativas a los sistemas asociados.	Asegurar la mejor alternativa para cumplir con los requerimientos.
SA3	Análisis de seguridad de alternativas encontradas	Alinear los objetivos de seguridad con los requisitos de seguridad.
SA4	Determinar el modelo medioambiental y el alcance.	Concretar la arquitectura de seguridad.
SA5	Análisis de riesgos de la ciudad inteligente	Analizar los riesgos de seguridad derivados de la implantación.

D. Diseño Seguro e Implementación (DI)

El Diseño e Implementación Segura de ciudades inteligentes corresponde al dominio de "Adquisición e implementación" de COBIT, pero con algunos cambios, en cuanto a los procesos que lo forman, así como la inclusión de nuevos procesos. Los cambios y la inclusión de los diferentes procesos tienen el objetivo de crear un marco de gobierno menos genérico. Este dominio pretende cubrir la fase de diseño e implementación de la ciudad inteligente. Este dominio está formado por 10 procesos que se explican en la Tabla V.

Tabla V:
PROCESOS DE DISEÑO SEGURO E IMPLEMENTACIÓN (DI)

Id	Proceso	Objetivo
DI1	Establecer roles y responsab. seguridad	Establecer un documento detallado con las responsabilidades de seguridad.
DI2	Adquirir y mantener los sistemas	Proporcionar los sistemas necesarios para apoyar el correcto funcionamiento.
DI3	Adquirir y mantener la infraestructura	Proporcionar la infraestructura necesaria para el funcionamiento.
DI4	Proporcionar los recursos necesarios	Para mejorar la rentabilidad.
DI5	Gestionar los cambios	Minimizar las pérdidas de tiempo que producen los cambios en la ciudad.
DI6	Diseñar controles de seguridad aplicables.	Definir las medidas o controles de seguridad que requiere la ciudad.
DI7	Implementación segura	Conseguir una implantación segura de la ciudad inteligente.
DI8	Instalar y acreditar cambios en la política de seguridad.	Verificar y confirmar que las nuevas políticas de seguridad se implementan adecuadamente en la ciudad inteligente.
DI9	Implementación segura de las telecomunicaciones	Asegurar la adecuada implementación de las diferentes medidas para proteger las tecnologías de las comunicaciones.
DI10	Implantación del centro de mando y control de la ciudad inteligente	Implementar adecuadamente el centro de mando y control de la ciudad inteligente.

Tabla VI:
AMENAZAS QUE PUEDEN AFECTAR A DOMINIOS EN SMART CITY

	Dominios	[C]	[D]	[I]
Economía	Economía	Robo de información confidencial Chantajear Pérdida de reputación	Colapso económico Arruinado	Quiebra Fraude en transacciones
M. Ambiente	M. Ambiente	Perfilado	Contaminación	Contaminación Destrucción HW
	Gestión energética	Perfilado	Apagón Problemas derivados en otros dominios.	Apagón Problemas derivados en otros dominios. Fraude
	Residuos		Contaminación	Contaminación Destrucción HW
Movilidad	Movilidad	Patrones de comportamiento Perfilado	Aislamiento Embotellamiento Escasez de conceptos básicos	Aislamiento Caos de tráfico
	Servicios de seguridad y emergencia.	Robo información confidencial Chantajear Secuestro	Muerte Confusión Fuego Inundación	Muerte Robo
Gobierno	Gobierno	Robo identid. Chantaje	Caos burocrático Pérdida reputación	Robo identidad Fraude
	Servicios sociales	Robo Inf. Confidencial Perfilado Chantaje Pérdida reputación	Cambios descendentes Enfermedad Escasez básica	Fraude Pérdida de reputación
Gente	Telecomunicaciones y medios	Perfilado Chantaje robo de información confidencial	Aislamiento Pérdida de reputación	Pérdida de reputación Manipulación de medios Engañoso

	Edificios	Patrones de comportamiento Robo Perfilado Chantaje Robo Inf. Confidencial Robo identidad	Robo Los planes de emergencia fallan Los controles de acceso fallan	Robo Los planes de emergencia fallan Los controles de acceso fallan Pérdidas económicas
Vivienda	Viviendas	Patrones de comportamiento Perfilado Robo Robo identidad	Aislamiento Cambios descendentes	Aislamiento Robo identidad Funcionamiento defectuoso
	Educación	robo de información confidencial Pérdida reputación	Cambios descendentes	Fraude Engañoso
	Salud	Robo Inf. Confidencial Perfilado Chantaje Pérdida reputación	Muerte Enfermedad	Muerte Enfermedad Fraude

Tabla VII:
PROCESOS DE OPERACIÓN SEGURA (SO)

Id	Proceso	Objetivo
SO1	Definir y gestionar niveles de seguridad.	Establecer un entendimiento mutuo del nivel de seguridad requerido.
SO2	Gestionar la seguridad de los servicios de terceros.	Garantizar que se definan y cumplan las responsabilidades en materia de seguridad de terceros.
SO3	Gestión de la eficiencia de la seguridad	Garantizar que se consiga la eficiencia de seguridad prevista. Para lograr esa capacidad y controles de desempeño se deben implementar.
SO4	Garantizar la disponibilidad total	Certificar que los diferentes servicios que forman la ciudad inteligente están siempre disponibles. Este proceso es especialmente importante en un escenario de ciudad inteligente.
SO5	Identificar y asignar desembolsos.	Garantizar el conocimiento de todos los costes derivados de la seguridad en la ciudad inteligente.
SO6	Formación del personal en ciudades inteligentes	Lograr que los usuarios sean conscientes de los riesgos y responsabilidades que se derivan de la ciudad inteligente y de cómo gestionarla.
SO7	Capacitación en seguridad del personal.	Garantizar que los usuarios hagan un uso seguro de las posibilidades de la ciudad inteligente.
SO8	Asistencia de seguridad	Garantizar que cualquier problema de seguridad ea debidamente atendido.
SO9	Gestión de configuración	Establecer y mantener un repositorio de configuración completo para garantizar la seguridad del sistema.
SO10	Gestionar problemas de seguridad	Para garantizar que se solucionen los problemas de seguridad.
SO11	Gestionar la seguridad de los datos	Certificar la seguridad de los datos durante el tratamiento de los mismos.
SO12	Gestionar la privacidad de datos	Garantizar la privacidad de los datos durante el tratamiento de los mismos.
SO13	Gestione la seguridad en el centro de comando y control	Proporcionar un control seguro sobre las actividades y datos gestionados en el centro de mando y control.
SO14	Gestionar la seguridad en las telecomunicaciones.	Para ofrecer una seguridad adecuada a las comunicaciones relacionadas con la ciudad inteligente,
SO15	Gestionar la seguridad física	Proporcionar un entorno físico seguro para proteger al personal y al equipo de amenazas naturales o humanas.
SO16	Gestionar operaciones seguras	Garantizar que las importantes funciones de seguridad se aborden de forma constante y adecuada.
SO17	Gestionar la continuidad de la ciudad inteligente	Crear un plan de continuidad específico en caso de que falle algún sistema de la ciudad inteligente.
SO18	Evaluación y adaptación del marco legal	Garantizar que el marco legal de la ciudad inteligente siga abordando los problemas de la ciudad.

Este dominio contiene el proceso DI6 sobre el diseño de diferentes controles de seguridad que se pueden aplicar a una ciudad inteligente. Para facilitar el desarrollo de estos controles, hemos creado una recopilación de los impactos que la materialización de una amenaza puede provocar en los diferentes ámbitos de una ciudad inteligente. Hemos dividido este conjunto de amenazas en las tres características de seguridad típicas: confidencialidad (C), disponibilidad (D) e integridad (I). El resultado de este estudio se muestra en la Tabla VI.

E. Funcionamiento de la seguridad (SO)

El dominio Operación Segura de ciudades inteligentes busca abordar cómo se gestiona la seguridad y privacidad de una ciudad inteligente, una vez que se han implementado los sistemas que la componen. En este caso, la mayoría de los procesos que se encuentran en este dominio son adaptaciones de procesos ya presentes en COBIT. Este dominio es probablemente el más importante en materia de seguridad porque aborda cómo funciona la ciudad inteligente y cómo se aprovechan los beneficios derivados del uso de esta tecnología. Este dominio está formado por 18 procesos diferentes explicados en la Tabla VII.

F. Monitoreo y Evaluación (ME)

El dominio de Monitoreo y Evaluación tiene como objetivo evaluar el desempeño de los sistemas en términos de indicadores de seguridad, y también incluye un proceso de auditoría externa. Respecto a COBIT, este dominio añade el proceso de realización de auditorías y adapta el resto de los procesos para alinearlos con el plan estratégico de seguridad establecido en el primer dominio. Este dominio está formado por 4 procesos diferentes explicados en la Tabla VIII.

Tabla VIII:
PROCESOS DE SEGUIMIENTO Y EVALUACIÓN (ME)

Id	Proceso	Objetivo
ME1	Monitorear y evaluar el desempeño de seguridad	Velar que se alcancen los objetivos preestablecidos para los proc. seg.
ME2	Monitorear y evaluar controles de seg. internos.	Garantizar el cumplimiento de los controles internos de seguridad.
ME3	Garantizar el cumplimiento legal	Garantizar el cumplimiento de los requisitos legales.
ME4	Implementación de auditorías de seguridad	Incrementar el nivel de confianza de la ciudad inteligente.

IV. CONCLUSIONES Y TRABAJO FUTURO

Este artículo expone la necesidad de crear un marco de gobierno de seguridad en ciudades inteligentes que pueda abordar el problema de la seguridad. Para lograr este objetivo se ha creado una propuesta de marco de seguridad de gobierno en entornos de ciudades inteligentes denominado SGSC. Las ciudades inteligentes y las tecnologías relacionadas con ellas todavía están evolucionando, por lo que para crear un marco completamente operativo es obligatorio realizar una investigación profunda para tener la base adecuada para construir nuestro marco.

Este acercamiento inicial al framework basa su estructura en COBIT pero provoca cambios significativos en algunos puntos fundamentales. Nuestro marco propuesto se divide en seis dominios principales que, al mismo tiempo, se componen de 56 procesos relacionados con la seguridad de las ciudades inteligentes. Además, estos procesos de seguridad se han creado mediante un estudio de las diferentes vulnerabilidades y ataques que puede sufrir una ciudad inteligente.

Finalmente, como trabajo futuro, nos gustaría expresar la necesidad de definir los diferentes controles y actividades que

forman cada uno de los procesos, los cuales deben ser específicos de las ciudades inteligentes. Para definir dichos controles y actividades, hemos considerado agregar buenas prácticas de diferentes modelos o estándares internacionales como CMMI. Además, tenemos la intención de crear cuadros de mando y herramientas de visualización para facilitar el seguimiento de los controles de seguridad en una ciudad inteligente.

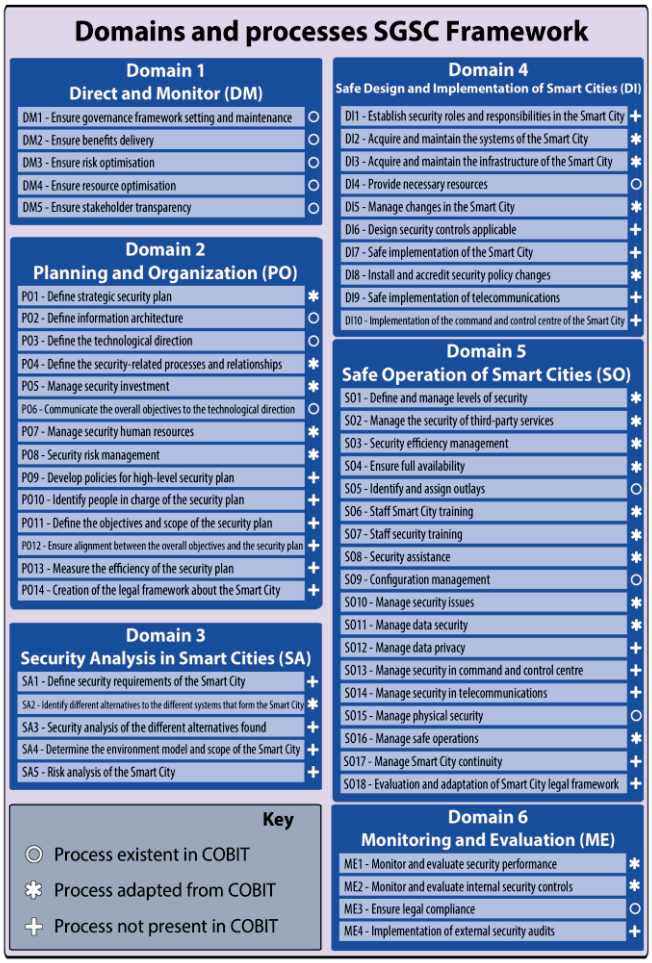

Fig 2. Dominios y procesos del marco SGSC.

AGRADECIMIENTOS

Este trabajo ha sido financiado por los proyectos Di4SPDS (subvención CHIST-ERA - PCI2023145980-2) financiado por MCIN/AEI y cofinanciado por la Unión Europea; AETHER-UCLM (PID2020-112540RB-C42) financiado por MCIN/AEI; ALBA-UC (TED2021-130355B-C33) y ALBA-UCLM (TED2021-130355B-C31) financiados por MICIU/AEI /10.13039/501100011033 y la Unión Europea NextGenerationEU/PRTR; y MESIAS (2022-GRIN-34202) financiado por FEDER.

REFERENCIAS

[1] Camero, A. and E. Alba, *Smart City and information technology: A review.* Cities, 2019. **93**: p. 84-94.

[2] Hussain, I., *Secure, Sustainable Smart Cities and the Internet of Things: Perspectives, Challenges, and Future Directions.* Sustainability, 2024. **16**(4): p. 1390.

[3] Almalki, F.A., et al., *Green IoT for Eco-Friendly and Sustainable Smart Cities: Future Directions and Opportunities.* Mobile Networks and Applications, 2023. **28**(1): p. 178-202.

[4] Sinimole, K. and S.L. Karri, *Security and Privacy Issues in Smart Cities*, in *Handbook of Artificial Intelligence for Smart City Development*. 2024, CRC Press. p. 228-248.

[5] GVR, *Smart Cities Market Size, Share & Trends Analysis Report By Application, By Smart Governance, By Smart Utilities, By Smart Transportation, By Smart Healthcare, By Region, And Segment Forecasts, 2024 - 2030*, in *Grand View Research*. 2023.

[6] Kiss, B., et al., *Citizen participation in the governance of nature-based solutions.* Environmental Policy and Governance, 2022. **32**(3): p. 247-272.

[7] De Felice, F., I. Baffo, and A. Petrillo, *Critical Infrastructures Overview: Past, Present and Future.* Sustainability, 2022. **14**(4): p. 2233.

[8] Djenna, A., S. Harous, and D.E. Saidouni, *Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure.* Applied Sciences, 2021. **11**(10): p. 4580.

[9] Badii, C., et al., *Smart City IoT Platform Respecting GDPR Privacy and Security Aspects.* IEEE Access, 2020. **8**: p. 23601-23623.

[10] Dobson, J.E. and W.A. Herbert, *Geoprivacy, Convenience, and the Pursuit of Anonymity in Digital Cities*, in *Urban Informatics*, W. Shi, et al., Editors. 2021, Springer Singapore: Singapore. p. 567-587.

[11] Zainuddin, N., et al. *A Study on Privacy Issues in Internet of Things (IoT)*. in *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*. 2021.

[12] Cohn, B.L., *Data Governance: A Quality Imperative in the Era of Big Data, Open Data and Beyond Symposium: Big Data Future Part One.* I/S: A Journal of Law and Policy for the Information Society, 2014. **10**(3): p. 811-826.

[13] Audit, I.S. and C. Association, *Cobit 5 A Business Framework for the Governance and Management of Enterprise*. 2012: ISACA.

[14] Eckhoff, D. and I. Wagner, *Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions.* IEEE Communications Surveys & Tutorials, 2018. **20**(1): p. 489-516.

[15] Demertzi, V., S. Demertzis, and K. Demertzis, *An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities.* Applied Sciences, 2023. **13**(2): p. 790.

[16] Murgante, B. and G. Borruso, *Smart Cities in a Smart World*, in *Future City Architecture for Optimal Living*, S.T. Rassia and P.M. Pardalos, Editors. 2015, Springer International Publishing: Cham. p. 13-35.

[17] Sharif, R.A. and S. Pokharel, *Smart City Dimensions and Associated Risks: Review of literature.* Sustainable Cities and Society, 2022. **77**: p. 103542.

[18] Toh, C.K., *Security for smart cities.* IET Smart Cities, 2020. **2**(2): p. 95-104.

[19] Ma, C., *Smart city and cyber-security; technologies used, leading challenges and future recommendations.* Energy Reports, 2021. **7**: p. 7999-8012.

[20] Kitchin, R. and M. Dodge, *The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention*, in *Smart cities and innovative Urban technologies*. 2020, Routledge. p. 47-65.

[21] Dodge, M. and R. Kitchin, *The challenges of cybersecurity for smart cities*, in *Creating Smart Cities*. 2018, Routledge. p. 205-216.

[22] Lévy-Bencheton, C., et al., *Cyber security for smart cities—An architecture model for public transport.* European Union Agency for Network and Information Security (ENISA), Tech. Rep, 2015.

[23] Cerrudo, C., *An emerging US (and world) threat: Cities wide open to cyber attacks.* Securing Smart Cities, 2015. **17**(2015): p. 137-151.

[24] Ahmad, T. and D. Zhang, *Using the internet of things in smart energy systems and networks.* Sustainable Cities and Society, 2021. **68**: p. 102783.

[25] Pliatsios, D., et al., *A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics.* IEEE Communications Surveys & Tutorials, 2020. **22**(3): p. 1942-1976.

[26] Ammara, U., et al., *Smart Cities from the Perspective of Systems.* Systems, 2022. **10**(3): p. 77.

[27] Puliafito, A., et al., *Smart Cities of the Future as Cyber Physical Systems: Challenges and Enabling Technologies.* Sensors, 2021. **21**(10): p. 3349.

[28] Ahmad, M.O., et al., *Cyber-Physical Systems and Smart Cities in India: Opportunities, Issues, and Challenges.* Sensors, 2021. **21**(22): p. 7714.

[29] Elassy, M., et al., *Intelligent transportation systems for sustainable smart cities.* Transportation Engineering, 2024. **16**: p. 100252.

[30] Kaššaj, M. and T. Peráček, *Synergies and Potential of Industry 4.0 and Automated Vehicles in Smart City Infrastructure.* Applied Sciences, 2024. **14**(9): p. 3575.

[31] Mohanty, R. and B.P. Kumar, *7 - Urbanization and smart cities*, in *Solving Urban Infrastructure Problems Using Smart City Technologies*, J.R. Vacca, Editor. 2021, Elsevier. p. 143-158.

[32] Rao, P.M. and B.D. Deebak, *Security and privacy issues in smart cities/industries: technologies, applications, and challenges.* Journal of Ambient Intelligence and Humanized Computing, 2023. **14**(8): p. 10517-10553.

[33] Framework, S.C., *Guide to establishing strategies for smart cities and communities.* BSI Standard PAS, 2014. **181**.