

Clausulado de seguridad para la contratación pública de tecnologías IoT en Smart Cities

Noviembre de 2025

Versión 1.0



Junta de Andalucía

Objeto del Expediente:

**“ELABORACIÓN DE GUÍAS DE CIBERSEGURIDAD IOT PARA ENTORNOS DE SMART CITIES Y SALUD”
(CONTR 2024 829153).**

Esta guía forma parte de la colección Guías de Ciberseguridad en IoT para las Smart Cities y el sector Salud creada por la Agencia Digital de Andalucía como parte del Proyecto Red Argos, perteneciente al programa RETECH, de Redes Inteligentes de Especialización Tecnológica, en el marco del Plan de Recuperación, Transformación y Resiliencia, financiado por la Unión Europea-NextGenerationEU, a través de INCIBE.

Autor del documento: Agencia Digital de Andalucía

Tipo de documento: Guía

Fecha de elaboración: 18/11/2025

Fecha de última actualización: 18/11/2025

ÍNDICE DE CONTENIDOS

1. Introducción	9
2. Objetivo y alcance	9
2.1. Objetivo	9
2.2. Alcance	10
3. Marco regulatorio	10
4. Definiciones	11
5. Instrucciones de uso.....	13
6. Tipologías de proveedores de tecnologías IoT en Smart Cities.....	14
6.1. Suministradores de dispositivos IoT	14
6.2. Prestadores de servicios IoT.....	14
6.3. Proveedores mixtos	15
7. Cláusulas de ciberseguridad para dispositivos IoT en Smart Cities	16
7.1. D_01 Gobernanza.....	16
7.1.1. C_01_01 Asignación de Responsabilidades	16
7.1.2. C_01_02 Políticas y procedimientos	17
7.1.3. C_01_03 Gestión Documental	17
7.2. D_02 Cumplimiento normativo	17
7.2.1. C_02_01 Normativa y conformidad.....	18
7.3. D_03 Gestión de usuarios y control de accesos.....	18
7.3.1. C_03_01 Sistemas de Control de Acceso y Autenticación	18
7.3.2. C_03_02 Procedimientos de Autorización de Acceso	19
7.4. D_04 Gestión del acceso remoto para servicios de mantenimiento	19
7.4.1. C_04_01 Autorización Previa para Herramientas de Acceso Remoto.....	19
7.4.2. C_04_02 Uso de Servicios VPN.....	20
7.4.3. C_04_03 Autenticación Multifactor	20
7.4.4. C_04_04 Autorización de Usuarios	20
7.4.5. C_04_05 Propuesta de Herramientas de Acceso Remoto para el Adjudicatario	21
7.4.6. C_04_06 Evaluación Excepcional de Herramientas de Acceso Remoto	21
7.5. D_05 Gestión de activos OT	21
7.5.1. C_05_01 Clasificación de Activos OT	22
7.5.2. C_05_02 Inventario de Activos.....	22

7.5.3.	C_05_03 Control de Alta, Baja y Modificación de Activos.....	22
7.6.	D_06 Configuración segura	22
7.6.1.	C_06_01 Configuración Inicial Segura.....	23
7.6.2.	C_06_02 Deshabilitación de Servicios.....	23
7.7.	D_07 Actualizaciones de software.....	23
7.7.1.	C_07_01 Políticas de Actualización	23
7.7.2.	C_07_02 Actualizaciones Automáticas.....	24
7.7.3.	C_07_03 Mecanismos Seguros de Actualización	24
7.7.4.	C_07_04 Evaluación de Impacto y Pruebas	24
7.7.5.	C_07_05 Documentación y Notificación	24
7.8.	D_08 Gestión de vulnerabilidades.....	24
7.8.1.	C_08_01 Proceso de Identificación y Gestión de Vulnerabilidades	25
7.8.2.	C_08_02 Análisis Regular de Vulnerabilidades	25
7.8.3.	C_08_03 Notificación y Plan de Corrección	25
7.8.4.	C_08_04 Implantación inicial libre de vulnerabilidades	26
7.9.	D_09 Desarrollo seguro.....	26
7.9.1.	C_09_01 Seguridad desde el diseño.....	26
7.10.	D_10 Mantenimiento físico de los dispositivos.....	27
7.10.1.	C_10_01 Coordinación con el equipo técnico y operativo	27
7.11.	D_11 Acceso de emergencia autorizado al dispositivo	27
7.11.1.	C_11_01 Mecanismo de Acceso de Emergencia.....	27
7.12.	D_12 Seguridad contra el código dañino.....	28
7.12.1.	C_12_01 Uso de software de protección contra código dañino.....	28
7.13.	D_13 Capacidad de bloqueo del dispositivo.....	29
7.13.1.	C_13_01 Niveles de Bloqueo Configurables.....	29
7.14.	D_14 Gestión de eventos	29
7.14.1.	C_14_01 Registros de Seguridad y Configuración de Logs.....	29
7.14.2.	C_14_02 Monitorización Continua y Revisión de Auditoría.....	30
7.15.	D_15 Gestión de incidentes	30
7.15.1.	C_15_01 Proceso Integral de Gestión de Incidentes.....	30
7.15.2.	C_15_02 Procedimientos de Contención y Recuperación.....	31
7.15.3.	C_15_03 Notificación de Incidentes	31
7.15.4.	C_15_04 Canales de Comunicación para Incidentes	31

7.16. D_16 Gestión segura de la cadena de suministro.....	32
7.16.1. C_16_01 Evaluación de Terceros Proveedores relacionados con la adjudicación.....	32
7.16.2. C_16_02 Contratos y Acuerdos.....	32
7.17. D_17 Gestión de la obsolescencia	33
7.17.1. C_17_01 Planificación de la Restitución y Transferencia Tecnológica	33
7.18. D_18 Protección de los servicios Cloud	33
7.18.1. C_18_01 Localización y Ubicación Geográfica de los Datos Personales.....	33
7.19. D_19 Continuidad de negocio	34
7.19.1. C_19_01 Procedimientos de Respaldo y Recuperación	34
7.19.2. C_19_02 Plan de Recuperación ante Contingencias	34
7.20. D_20 Auditorías técnicas y de cumplimiento	35
7.20.1. C_20_01 Requisitos de Pruebas de Seguridad.....	35
7.20.2. C_20_02 Capacidad para Pruebas de Seguridad y Auditorías.....	35
7.20.3. C_20_03 Pruebas de Validación Post-Despliegue.....	36
7.21. D_21 Formación y concienciación en ciberseguridad.....	36
7.21.1. C_21_01 Programas de Formación.....	36
7.21.2. C_21_02 Concienciación de Seguridad	37
7.22. D_22 Protección física de los dispositivos	37
7.22.1. C_22_01 Protección Física de los Dispositivos.....	37
7.23. D_23 Comunicaciones seguras.....	38
7.23.1. C_23_01 Configuración de Redes y Comunicaciones	38
7.24. D_24 Segmentación de la red urbana desplegada	38
7.24.1. C_24_01 Segmentación por criticidad y función	39
7.24.2. C_24_02 Comunicaciones seguras y servicios expuestos	39
7.24.3. C_24_03 Protección de segmentos inalámbricos y redes municipales	39
7.25. D_25 Protección de la información	40
7.25.1. C_25_01 Medidas de Seguridad para la Protección de Datos	40
7.26. D_26 Interoperabilidad segura con microservicios.....	40
7.26.1. C_26_01 Configuración segura de APIs	41
7.27. D_27 Protección de los soportes de información	41
7.27.1. C_27_01 Devolución y Destrucción de Datos	41
7.28. D_28 Integración segura con aplicaciones móviles.....	42
7.28.1. C_28_01 Permisos y funcionalidades limitadas.....	42

7.28.2. C_28_02 Restricción de distribución de la aplicación en markets no autorizados	42
7.29. D_29 Integración con los Centro de Control Urbano o Plataforma Ciudad Inteligente.....	43
7.29.1. C_29_01 Interfaces e interoperabilidad	43
7.29.2. C_29_02 Seguridad en la integración	43
7.29.3. C_29_03 Monitorización y gestión centralizada	43
7.30. D_30 Tratamiento de la información	44
7.30.1. C_30_01 Transferencia de Conocimiento e Información al Finalizar el Contrato	44
8. Anexos.....	45
8.1. Anexo I: Guía para la clasificación de la criticidad de dispositivos y sistemas IoT.....	45
8.1.1. Introducción al modelo CIDAT.....	45
8.1.2. Procedimiento para la clasificación	45
8.1.3. Ejemplos ilustrativos.....	46
8.2. Anexo II: Relación entre tipología de proveedores y clausulado	47
9. Referencias y enlaces a información adicional	55
10. Otras referencias de interés	56
10.1. Lista de materias tratadas en la guía	56
10.2. Lista de productos mencionados en al guía	56
10.3. Lista de servicios mencionados en la guía	56

ÍNDICE DE TABLAS

Tabla 1: Definiciones empleadas.	13
Tabla 2: Mapeo de tipología de proveedores con los dominios/cláusulas.	54

ÍNDICE DE FIGURAS

Ilustración 1: Metodología de interpretación de la guía.	14
---	----

1. Introducción

El despliegue de tecnologías basadas en Internet of Things (en adelante, IoT) dentro de las Smart Cities ha experimentado un crecimiento exponencial en los últimos años. Estas tecnologías permiten optimizar la movilidad, mejorar la gestión de recursos, potenciar la seguridad de los ciudadanos y ofrecer servicios urbanos más eficientes. No obstante, la implementación masiva de dispositivos conectados también lleva consigo desafíos relevantes en el ámbito de la ciberseguridad, interoperabilidad, protección de datos personales y resiliencia de los sistemas, dado que gran parte de la información que circula resulta crítica para el correcto funcionamiento de los servicios urbanos y la confianza de la ciudadanía en esta tecnología.

En el presente documento se establecen las cláusulas de seguridad aplicables para procesos de contratación pública que contemplen la adquisición, implementación, operación o integración de tecnologías IoT aplicadas a entornos urbanos. El objetivo es definir criterios técnicos y normativos que aseguren que proveedores y adjudicatarios adopten medidas de seguridad desde el diseño, gestión de riesgos y vulnerabilidades, asignación de roles y responsabilidades claras, en cada una de las fases del ciclo de vida de los dispositivos y servicios.

Es de mencionar, que las cláusulas recogidas en el documento son de obligado cumplimiento para los adjudicatarios y deberán integrarse en los pliegos técnicos vinculados a proyectos de IoT en Smart Cities. Su aplicación permitirá fortalecer la seguridad de los entornos urbanos conectados frente a posibles incidentes que puedan poner en riesgo la disponibilidad, integridad o confidencialidad de los datos tratados.

2. Objetivo y alcance

2.1. Objetivo

El propósito del presente documento es apoyar a los órganos de contratación en la incorporación de cláusulas de ciberseguridad en los pliegos técnicos relacionados con dispositivos, sistemas y servicios IoT en los entornos de Smart Cities. A través de un enfoque estructurado por dominios, permitiendo seleccionar requisitos contractuales ajustados al tipo de solución, proveedor y criticidad funcional del dispositivo o servicio objeto del contrato.

Los objetivos que se presentan a continuación definen el propósito general del documento y orientan su uso práctico en los distintos procedimientos de contratación:

- Establecer un marco común y homogéneo de cláusulas técnicas de ciberseguridad aplicables a la contratación de tecnologías IoT en entornos urbanos inteligentes, alineado con la normativa vigente y los principales estándares nacionales e internacionales en materia de protección de datos, seguridad de la información y gestión de riesgos tecnológicos.
- Facilitar a los órganos de contratación pública la inclusión de requisitos de seguridad adecuados, proporcionados y verificables, adaptados al tipo de servicio IoT prestado bajo el objeto del contrato.

- Minimizar los riesgos derivados de la integración de tecnologías IoT en las infraestructuras urbanas, garantizando el cumplimiento de principios como la seguridad desde el diseño, la privacidad por defecto, la trazabilidad, la interoperabilidad segura y la resiliencia operativa.
- Impulsar la responsabilidad compartida en materia de la ciberseguridad de los entornos urbanos entre entidades públicas y adjudicatarios.
- Favorecer el cumplimiento de las normativas y estándares en el ámbito.

2.2. Alcance

El clausulado incorporado en el presente documento es aplicable a todos los dispositivos, sistemas y servicios relacionados con IoT que se adquieran, desplieguen o mantengan en el ámbito del sector urbano. Esto incluye, entre otros, sensores y actuadores urbanos, pasarelas de comunicaciones, plataformas de monitorización y gestión, aplicaciones móviles de servicios públicos, servicios en la nube y cualquier otro componente o servicio que forme parte de la cadena tecnológica y operativa del ecosistema IoT objeto de licitación.

La aplicación de las cláusulas de seguridad se adaptará al nivel de criticidad del activo y a la tipología del proveedor, de forma que las medidas resulten proporcionales al riesgo y con lo establecido en las regulaciones y normativas aplicables.

3. Marco regulatorio

El presente documento se fundamenta en un marco regulador amplio que combina normativa legal, estándares técnicos y guías de buenas prácticas, a fin de asegurar el cumplimiento y alineación con las exigencias del sector urbano.

- **Normativas:**
 - Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales (en adelante, CRA).
 - Reglamento (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativo a las medidas para asegurar un alto nivel común de ciberseguridad en la UE (en adelante, NIS2).
 - Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (en adelante, RGPD).
 - Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS).
 - Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD).
- **Estándares:**
 - IEC 62443, Seguridad para sistemas de automatización y control industrial.
 - ISO/IEC 27400, Seguridad y privacidad en IoT.
 - ISO/IEC TR 23188:2020, Ecosistemas de Edge Computing.
 - ISO/IEC 27001, Gestión de la seguridad de la información.

- ISO/IEC 27701, Privacidad de la información.
- ISO/IEC 27017 y 27018, Seguridad y privacidad en servicios cloud.
- ISO/IEC 24518, Gestión de crisis en el suministro de agua.
- ISO/IEC 22301, Gestión de la continuidad de negocio.
- ISO/IEC 50001, Gestión del suministro eléctrico.
- **Guías:**
 - Cloud Security Alliance (CSA), Matriz de controles Cloud (CCM).
 - ENISA, Guía para la securización de IoT.
 - Guías CCN-STIC del Esquema Nacional de Seguridad (811, 823, 824, 881, 891).
 - Guía NIST SP 800-53 y SP 800-115 (controles y pruebas técnicas de seguridad).
 - NIST IR 8259 Serie, Guía de Ciberseguridad para fabricantes de dispositivos IoT.
 - NIST SP 800-213 Serie, Guía de Ciberseguridad para dispositivos IoT.
 - OWASP IoT y OWASP, Guías de auditorías técnicas.

4. Definiciones

Acrónimos	Definición
Actor de amenazas	Individuo o grupo de ciberatacantes que representan un riesgo potencial para un sistema o red.
API	Conjunto de reglas que permiten que programas se comuniquen entre sí (del inglés, Application Programming Interface).
API Keys	Credenciales utilizadas para autenticar aplicaciones en una API (del inglés, Application Programming Interface Keys).
CIDAT	Dimensiones de seguridad de la información definidas por el ENS: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
CMDB	Base de datos que contiene información sobre los activos de TI (del inglés, Configuration Management Database).
CPSTIC	Catálogo de y productos de seguridad TIC certificados por el CCN-CERT en España.
Cifrado en reposo	Protección de datos almacenados mediante técnicas criptográficas.
Cifrado en tránsito	Protección de datos mientras se transmiten mediante técnicas criptográficas.
Código fuente	Conjunto de instrucciones escritas por un desarrollador en un lenguaje de programación.
Edge Computing	Procesamiento de datos cerca de su origen para reducir la latencia (del inglés, Edge Computing).
Escaneo	Análisis de sistemas para identificar puertos abiertos, servicios o vulnerabilidades.

Acrónimos	Definición
Firmware	Tipología de software integrado en dispositivos electrónicos que controla el hardware y permite su funcionamiento básico.
HTTP	Protocolo para la transferencia de páginas web (del inglés, Hypertext Transfer Protocol) por el puerto 80.
HTTPS	Versión segura del protocolo HTTP (del inglés, Hypertext Transfer Protocol Secure) por el puerto 443.
IP	Identificador único para dispositivos en una red (del inglés, Internet Protocol).
Ingeniería social	Manipulación psicológica para obtener acceso no autorizado o información.
Inteligencia de amenazas	Información que permite anticipar, detectar y responder a amenazas de seguridad.
Inyección SQL	Tipo de ataque que manipula consultas SQL para acceder o modificar datos.
JSON	Formato ligero de intercambio de datos legible por humanos y máquinas (del inglés, JavaScript Object Notation).
JSON Web Tokens (JWT)	Estándar abierto para transmitir datos de forma segura como objetos JSON.
Latencia	Tiempo que tarda un paquete de datos en viajar de origen a destino.
Logs	Registros que documentan eventos dentro de sistemas y aplicaciones.
LoRaWAN	Protocolo de comunicación inalámbrica de largo alcance, baja potencia y ancho de banda para IoT (del inglés, Low Power Wide Area Network).
MAC	Dirección física única asignada a una tarjeta de red de un dispositivo (del inglés, Media Access Control).
MFA	Método de autenticación que combina múltiples factores (del inglés, Multi-Factor Authentication).
Mínimo privilegio	Principio que limita los accesos al mínimo necesario para realizar tareas.
MQTT	Protocolo de mensajería ligero diseñado para redes con recursos limitados o inestables (del inglés, Message Queuing Telemetry Transport).
NB-IoT	Tecnología de comunicación inalámbrica de largo alcance y baja potencia para dispositivos IoT (del inglés, NarrowBand Internet of Things).
OGC SensorThings API	Estándar abierto del OGC (del inglés, Open Geospatial Consortium) para la interoperabilidad de datos de sensores IoT.
OPC-UA	Estándar de comunicación industrial independiente de la plataforma (del inglés, Open Platform Communications Unified Architecture).
OT	Tecnología operativa usada en entornos industriales para controlar procesos físicos.

Acrónimos	Definición
Perímetro tipo 6 (APP-6)	Designación del perímetro de seguridad que se aplica a aplicaciones según el ENS.
Pruebas de penetración	Simulación controlada de ataques para identificar vulnerabilidades.
Puertos	Puntos lógicos de conexión para enviar o recibir datos en una red.
Registros de auditoría	Logs utilizados para seguimiento de actividades, accesos y cambios en sistemas.
REST	Arquitectura para sistemas distribuidos centrada en el intercambio de información a través de HTTP (del inglés, Representational State Transfer).
Roles RBAC	Modelo de control de acceso basado en roles (del inglés, Role-Based Access Control).
Rollback	Proceso de revertir un sistema a un estado anterior tras un fallo o error.
SDLC	Proceso estructurado para el desarrollo de software (del inglés, Software Development Life Cycle).
SIEM	Plataforma que centraliza y analiza eventos de seguridad (del inglés, Security Information and Event Management).
Superficie de ataque	Conjunto de puntos o vectores por donde un atacante o actor de amenazas puede intentar acceder a un sistema o entorno.
Syslog	Protocolo estándar para el envío de mensajes de registro de sistemas.
TLS	Protocolo criptográfico que proporciona seguridad en las comunicaciones (del inglés, Transport Layer Security).
VPN	Tecnología que crea una conexión segura sobre una red pública (del inglés, Virtual Private Network).
Vulnerabilidad	Debilidad en un sistema que puede ser explotada por atacantes o actores de amenazas.
XML	Lenguaje de marcado usado para almacenar y transportar datos (del inglés, eXtensible Markup Language).

TABLA 1: DEFINICIONES EMPLEADAS.

5. Instrucciones de uso

El presente punto tiene como finalidad proporcionar una guía clara, estructurada y orientativa que permita realizar una selección coherente y conforme con la legislación vigente a los gestores encargados de redactar los pliegos de contratación pública relacionados con dispositivos, sistemas y servicios de IoT para el entorno urbano.

A continuación, se muestra de forma ilustrativa las instrucciones de uso de la correspondiente guía:

INSTRUCCIONES GUÍA CLAUSULADO IoT SMART CITIES

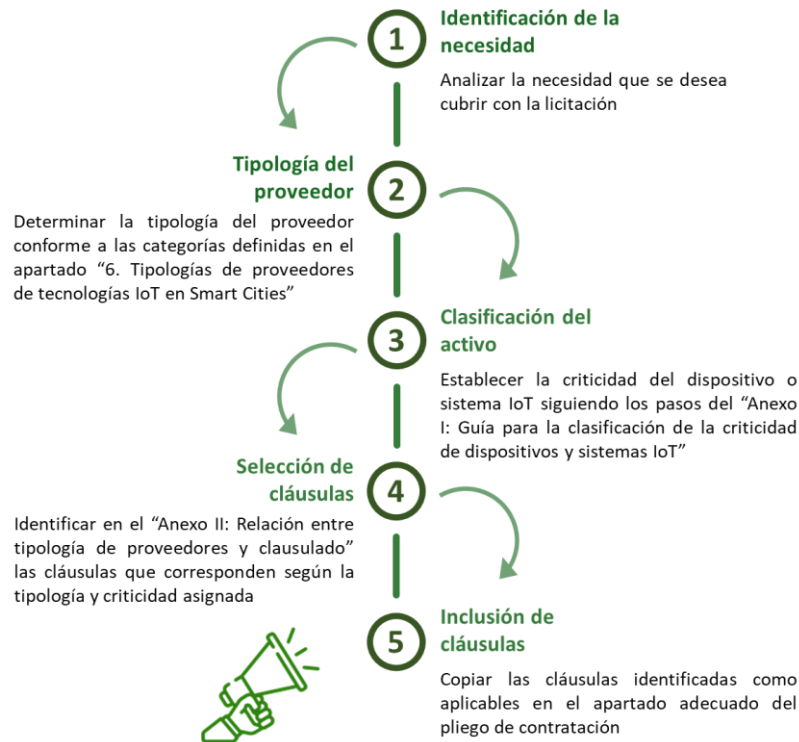


ILUSTRACIÓN 1: METODOLOGÍA DE INTERPRETACIÓN DE LA GUÍA.

6. Tipologías de proveedores de tecnologías IoT en Smart Cities

6.1. Suministradores de dispositivos IoT

Se entiende por suministradores de dispositivos IoT a aquellos proveedores **responsables del diseño, desarrollo, producción y comercialización de dispositivos conectados** que forman parte del ecosistema urbano.

Dichos fabricantes deben garantizar que sus productos cumplan con la normativa aplicable, incluyendo el **Reglamento (UE) 2024/2847 (CRA)**, así como los requisitos de seguridad y protección de datos personales definidos por el Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD).

También, son responsables de suministrar la documentación técnica del producto, proveer actualizaciones de firmware o software y comunicar cualquier riesgo o vulnerabilidad asociado a su uso.

6.2. Prestadores de servicios IoT

Se consideran prestadores de servicios los proveedores responsables de la **instalación, configuración inicial y mantenimiento de los dispositivos y sistemas IoT** relacionados con servicios urbanos, así como aquellos que ofrecen soporte técnico. Sus funciones incluyen la aplicación de actualizaciones de

seguridad, el reemplazo de componentes, la monitorización del estado de los equipos y la resolución de incidencias.

También forman parte de esta categoría los proveedores que ofrecen **servicios de análisis, gestión de datos y consultoría**, orientados a extraer valor operativo o estratégico a partir de la información generada por los dispositivos IoT. Entre sus actividades se incluyen la implementación de modelos analíticos, cuadros de mando y soluciones de inteligencia artificial, entre otras.

Por último, se incluyen dentro de esta tipología aquellos proveedores que ofrecen **capacidades de procesamiento, almacenamiento y gestión de datos** tanto en la **nube** como en entornos perimetrales (**Edge Computing**), siempre que **no** suministren **infraestructura propia**.

Todos los proveedores de esta tipología deberán garantizar que sus servicios cumplan con la normativa aplicable, incluyendo el **Real Decreto 311/2022**, de 3 de mayo, que regula el **Esquema Nacional de Seguridad**, así como con los requisitos de seguridad y protección de datos personales definidos por el Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD).

6.3. Proveedores mixtos

Se consideran proveedores de servicios mixtos aquellos que, además de **suministrar dispositivos IoT** del ecosistema urbano, asumen la prestación de **servicios asociados** que abarcan su instalación, configuración inicial, mantenimiento, soporte técnico y gestión operativa. Este tipo de proveedores combina las funciones propias de un **suministrador** con las de un **prestador de servicios**, lo que les confiere un rol integral en todo el ciclo de vida de los dispositivos.

Asimismo, también se incluyen en esta categoría aquellos proveedores que ofrecen **capacidades de procesamiento, almacenamiento y gestión de datos** tanto en la **nube** como en entornos perimetrales (**Edge Computing**), siempre que suministren y gestionen **infraestructura propia**.

Todos los proveedores de esta tipología deberán garantizar el cumplimiento normativo aplicable, incluyendo el **Reglamento (UE) 2024/2847 (CRA)** para los dispositivos conectados, el **Real Decreto 311/2022** que regula el **Esquema Nacional de Seguridad** para los servicios, así como el Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD), entre otros.

7. Cláusulas de ciberseguridad para dispositivos IoT en Smart Cities

El presente apartado recoge un conjunto estructurado de cláusulas de ciberseguridad organizadas por dominios funcionales. En este sentido, cada cláusula está diseñada para proporcionar principalmente requisitos de ciberseguridad que permitan mantener la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad (CIDAT) en los dispositivos, sistemas y servicios relacionados con IoT en Smart Cities a licitar.

7.1. D_01 Gobernanza

- **Definición del dominio**

Conjunto de mecanismos, roles, políticas y procesos que el adjudicatario debe definir e implementar para asegurar una gestión clara y estructurada de los entornos IoT urbanos. Esto implica establecer con claridad las responsabilidades de las partes involucradas, garantizar la existencia de políticas y procedimientos documentados que regulen el uso y supervisión de los sistemas de información, y velar porque toda la documentación se mantenga actualizada, organizada y accesible durante toda la vigencia del contrato.

Una gobernanza adecuada facilita la toma de decisiones y la correcta asignación de responsabilidades, especialmente en situaciones críticas como incidentes de seguridad o fallos operativos en los entornos IoT urbanos.

- **Cláusulas aplicables**

7.1.1. C_01_01 Asignación de Responsabilidades

El adjudicatario será responsable de definir, documentar y mantener actualizada una matriz de roles y responsabilidades específica para la gestión de la seguridad de los dispositivos, sistemas y servicios relacionados con IoT urbanos. Esta matriz deberá asignar claramente las funciones relacionadas el objeto del contrato, así como la gestión segura de dichos dispositivos. Además, deberá asignar un Punto Único de Contacto de Seguridad (POC), que actuará como interlocutor principal con la entidad pública para todas las comunicaciones relativas a la seguridad de la información y la gestión de incidentes, dando soporte en el cumplimiento de los requisitos de ciberseguridad aplicables.

Asimismo, cuando el adjudicatario asuma el mantenimiento y soporte de los entornos IoT, deberá designar un responsable técnico por cada entorno, proporcionando al POC los recursos necesarios para coordinar las acciones de respuesta ante incidentes, manteniendo así la integridad, confidencialidad y disponibilidad de los datos procesados por los dispositivos y servicios urbanos.

El adjudicatario garantizará que todos los roles asignados estén respaldados por la capacitación adecuada, documentación de procesos y mecanismos de supervisión periódica. Cualquier cambio en las responsabilidades deberá ser notificado y aprobado formalmente por la entidad contratante, asegurando una trazabilidad completa en la gestión de los activos IoT.

7.1.2. C_01_02 Políticas y procedimientos

El adjudicatario deberá desarrollar, implementar y mantener Sistema de Gestión de Seguridad de la Información (SGSI), o un conjunto formal de políticas y procedimientos, con alcance específico en los dispositivos, sistemas y servicios relacionados con IoT objeto del contrato. Dicho SGSI deberá estar alineado con los marcos regulatorios aplicables, las mejores prácticas de ciberseguridad, las normas específicas del entorno urbano, y el cuerpo normativo de la entidad contratante.

Las políticas incluidas deberán abordar, aspectos como configuración inicial, control de acceso, monitorización continua, gestión de vulnerabilidades, aplicación de parches, desactivación segura de funciones no necesarias y protección de datos personales procesados por los dispositivos, sistemas y servicios relacionados con IoT.

Los procedimientos asociados deberán ser detallados, operativos y actualizados regularmente, garantizando su alineación con las normativas de la entidad contratante.

Cualquier modificación en las políticas o procedimientos por parte del adjudicatario deberá ser debidamente registrada y aprobada por los órganos competentes del adjudicatario, comunicando a la entidad contratante aquellas variaciones que resulten relevantes para el objeto del contrato.

7.1.3. C_01_03 Gestión Documental

El adjudicatario será responsable de la elaboración, entrega y actualización de toda la documentación técnica y operativa relacionada con los dispositivos IoT suministrados o gestionados en el marco del presente contrato. Dicha documentación deberá incluir manuales de usuario, guías de instalación, protocolos de mantenimiento, instrucciones de seguridad, procedimientos de actualización, y cualquier otro documento necesario para el correcto uso, gestión y soporte de los dispositivos por parte de los operadores de servicios urbanos y el personal técnico.

Toda la documentación entregada a la entidad contratante deberá cumplir con los siguientes requisitos:

- Formato y lenguaje, la información deberá presentarse en un formato claro y estructurado, redactada en idioma español, utilizando un lenguaje técnico comprensible para operadores y técnicos.
- Accesibilidad, el adjudicatario deberá garantizar que toda la documentación pueda ser almacenada en un repositorio centralizado siguiendo los procedimientos y formatos establecidos por la entidad contratante, de forma que se asegure su correcta integración y disponibilidad para su posterior consulta por parte del personal autorizado.
- Actualización continua, la documentación deberá actualizarse durante toda la vigencia del contrato, incorporando cualquier cambio en configuraciones, versiones de software, funcionalidades o normativas aplicables.

7.2. D_02 Cumplimiento normativo

• Definición del dominio

El adjudicatario deberá garantizar el cumplimiento de todas las obligaciones legales, regulatorias y normativas aplicables en la prestación de servicios y/o suministro de dispositivos, sistemas y soluciones relacionados con el ecosistema IoT urbano. Esto incluye, entre otros, el cumplimiento del Esquema Nacional de Seguridad (ENS), en su versión vigente, para los servicios prestados, Reglamento (UE)

2024/2847 (CRA) para los dispositivos conectados suministrados, así como otros estándares y normativas aplicables en materia de ciberseguridad.

Asimismo, se deberá cumplir con normativas de protección de datos personales, como el Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD).

- **Cláusulas aplicables**

- 7.2.1. C_02_01 Normativa y conformidad**

El adjudicatario será responsable de garantizar que todos los dispositivos, sistemas y servicios relacionados con IoT suministrados o gestionados en el marco del presente contrato se encuentren plenamente adecuados a la normativa vigente en materia de ciberseguridad aplicable al sector urbano.

En el caso de dispositivos IoT, deberá acreditar que cuentan con marcado CE y que cumplen los requisitos establecidos en Reglamento (UE) 2024/2847 (CRA) o, cuando corresponda, en otros reglamentos o normativas de aplicación específica según el tipo de dispositivo y su uso previsto.

Asimismo, para el resto de los dispositivos y servicios asociados, el adjudicatario deberá aportar evidencias verificables que acrediten el cumplimiento de las obligaciones contractuales y normativas, como ENS, NIS2, RGPD y LOPDGDD, mediante certificaciones vigentes, informes de auditoría externa, pruebas de conformidad realizadas por terceros cualificados o, en su defecto, documentación técnica que demuestre la correcta aplicación de las medidas exigidas.

Por otro lado, deberá exigir a los técnicos que formen parte del equipo de trabajo objeto de este contrato el cumplimiento de la normativa de seguridad establecida por la entidad contratante en relación con las obligaciones y funciones del personal. El adjudicatario quedará obligado frente a la entidad por las responsabilidades que puedan derivarse del incumplimiento de esta normativa.

7.3. D_03 Gestión de usuarios y control de accesos

- **Definición del dominio**

Conjunto de controles y mecanismos que el adjudicatario debe implementar para asegurar que únicamente las personas autorizadas puedan acceder a los sistemas y servicios relacionados con el entorno IoT urbano, incluyendo sistemas de control de accesos y la definición de perfiles de usuario según su función o nivel de responsabilidad.

Además, deberán establecerse procedimientos internos formales para garanticen la notificación a la entidad contratante de la necesidad de cualquier alta, cambio o baja en los usuarios prestadores del servicio, permitiendo que dicho proceso sea gestionado por la entidad de forma segura y trazable.

- **Cláusulas aplicables**

- 7.3.1. C_03_01 Sistemas de Control de Acceso y Autenticación**

Los dispositivos, sistemas y servicios relacionados con IoT en el entorno urbano deberán disponer de un sistema de control de acceso robusto que garantice que únicamente el personal debidamente autorizado pueda acceder a las funcionalidades críticas de los dispositivos, así como a la información personal o sensible que estos procesen.

En caso de que el dispositivo o sistema lo permita, se deberán implementar controles de acceso basados en roles RBAC (del inglés, *Role Based Access Control*) de manera que las aplicaciones permitan el establecimiento de distintos grupos de usuarios en función de las actividades que realicen. Dichos grupos deberán estar identificados y detallados en base a los privilegios de los mismos y sus responsabilidades asociadas.

El adjudicatario tiene la obligación de establecer procedimientos internos formales para notificar oportunamente a la entidad contratante la necesidad de cualquier alta, modificación y/o baja de los usuarios prestadores de los servicios, garantizando que se lleve a cabo el bloqueo y posterior eliminación de las cuentas asociadas.

7.3.2. C_03_02 Procedimientos de Autorización de Acceso

Los mecanismos de control de acceso deberán estar alineados con los procedimientos establecidos por la entidad contratante para las autorizaciones de acceso a los dispositivos y sus sistemas de información relacionados.

Las políticas de acceso y autorización serán revisadas y actualizadas periódicamente por el adjudicatario para reflejar posibles cambios en el personal y las necesidades de seguridad, garantizando que solo el personal estrictamente necesario tenga acceso a la información sensible o a las funciones críticas de los sistemas.

La entidad contratante podrá llevar a cabo auditorías regulares y pruebas técnicas para asegurar el cumplimiento de los procedimientos de autorización de acceso y para identificar y corregir cualquier desviación detectada.

7.4. D_04 Gestión del acceso remoto para servicios de mantenimiento

• Definición del dominio

Conjunto de medidas que regulan cómo el adjudicatario puede acceder remotamente a los sistemas y dispositivos IoT urbanos para realizar tareas de mantenimiento, soporte o actualización. Este acceso deberá estar debidamente autorizado por la entidad contratante, y solo podrá realizarse a través de herramientas previamente evaluadas y aprobadas, incluyendo el uso obligatorio de servicios seguros como redes privadas virtuales (VPN) y mecanismos de autenticación multifactor.

• Cláusulas aplicables

7.4.1. C_04_01 Autorización Previa para Herramientas de Acceso Remoto

El adjudicatario no podrá utilizar herramientas o mecanismos de acceso remoto a los dispositivos, sistemas o plataformas vinculadas a soluciones IoT urbanas sin la autorización previa, expresa y por escrito de la entidad contratante. La autorización deberá solicitarse para cada herramienta específica, detallando su finalidad, alcance técnico, medidas de seguridad implementadas, trazabilidad de las acciones realizadas y el personal autorizado para su uso.

Ninguna herramienta de acceso remoto destinada a la prestación de servicios de mantenimiento o resolución de incidencias en los dispositivos y sistemas de información relacionados se considerará preautorizada sin la aprobación explícita de la entidad contratante.

7.4.2. C_04_02 Uso de Servicios VPN

El adjudicatario deberá utilizar exclusivamente los servicios corporativos de Red Privada Virtual (VPN) sede a sede proporcionados por la entidad contratante, o, en su defecto, aquellos que cuenten con autorización previa, expresa y por escrito por parte de la entidad antes de su uso.

Las soluciones empleadas deberán garantizar la confidencialidad, integridad y autenticación de las comunicaciones, así como cumplir con los requisitos técnicos y normativos aplicables en materia de seguridad y operatividad para el ámbito urbano. Todas las comunicaciones realizadas a través de la VPN deberán estar cifradas y autenticadas adecuadamente, empleando mecanismos de cifrado robustos y estándares actualizados.

La arquitectura y configuración de la VPN utilizada deberá alinearse con los principios del Esquema Nacional de Seguridad (ENS) o encontrarse incluida en el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información (CPSTIC) del CCN-CERT, siendo asimismo valorable su conformidad con estándares de seguridad reconocidos como ISO/IEC 27001 o equivalentes.

El adjudicatario será responsable de proporcionar la documentación técnica de la solución VPN propuesta, así como de garantizar su correcta operación, mantenimiento y actualización. Queda expresamente prohibido el uso de soluciones de conectividad no autorizadas, genéricas o de carácter comercial no controlado.

7.4.3. C_04_03 Autenticación Multifactor

Es obligatorio el uso de autenticación multifactor (en adelante, MFA) para todos los accesos remotos a los dispositivos, sus sistemas de información y los servicios relacionados con IoT por parte del adjudicatario, siempre que la arquitectura técnica lo permita. En caso de que las características técnicas del dispositivo o protocolo impidan la implementación de MFA, el adjudicatario deberá justificarlo y aplicar medidas alternativas equivalentes, conforme a las mejores prácticas reconocidas y a la normativa aplicable.

Además, los mecanismos de MFA implementados deberán ser avanzados y garantizar la verificación robusta de la identidad de los usuarios que acceden a los sistemas, asegurando la confidencialidad e integridad de la conexión.

El adjudicatario, en caso de que proporcione sus propias herramientas de acceso remoto o cuando lo requiera la entidad contratante, será responsable de garantizar su correcta configuración, mantenimiento y actualización, así como de registrar y conservar los logs de acceso de forma trazable y auditable.

No se permitirá el uso de credenciales compartidas ni de mecanismos de autenticación que no cumplan con los niveles de seguridad exigidos por la entidad contratante y la normativa aplicable.

7.4.4. C_04_04 Autorización de Usuarios

Solo los usuarios previamente autorizados por la entidad contratante a propuesta del adjudicatario tendrán los derechos de acceso necesarios para la prestación de servicios de mantenimiento y resolución de incidencias mediante acceso remoto a los dispositivos, sistemas y servicios relacionados con IoT en el entorno urbano.

7.4.5. C_04_05 Propuesta de Herramientas de Acceso Remoto para el Adjudicatario

El adjudicatario podrá proponer herramientas específicas de acceso remoto a dispositivos, sistemas y servicios relacionados con IoT urbano para la prestación de servicios de mantenimiento y resolución de incidencias.

Las soluciones de acceso remoto deberán respetar la arquitectura de seguridad de la entidad contratante, en particular, cuando sea posible, deberán cumplir con la arquitectura de protección de perímetro tipo 6 (APP-6) según lo establecido en la Guía de Seguridad TIC CCN-STIC 811.

No obstante, dado que las tecnologías de IoT urbano, como LoRaWAN, NB-IoT o redes celulares, presentan características de conectividad, topología y recursos diferentes a las redes corporativas tradicionales, se permitirá la utilización de arquitecturas y mecanismos de seguridad equivalentes, debidamente justificados y validados por la entidad contratante, que garanticen un nivel de protección comparable al exigido por APP-6.

7.4.6. C_04_06 Evaluación Excepcional de Herramientas de Acceso Remoto

En casos donde la herramienta propuesta por el adjudicatario no soporte la arquitectura de seguridad APP-6 o no pueda utilizar servicios de VPN, la entidad contratante podrá evaluar excepcionalmente el uso de otras herramientas propuestas por el adjudicatario. Asimismo, en caso de que dichas herramientas no resulten adecuadas, podrá considerarse la prestación de los servicios de forma presencial en las instalaciones de la entidad contratante, respetando en todo momento la normativa relativa al control de acceso físico.

Las herramientas podrán ser autorizadas únicamente si cumplen con las condiciones de seguridad requeridas y no incrementan el riesgo para la seguridad de las infraestructuras de la entidad contratante. Será responsabilidad del adjudicatario demostrar el cumplimiento de dichas condiciones mediante análisis y pruebas de seguridad realizados por terceros independientes acreditados, cuyos resultados deberán ser entregados a la entidad contratante para su verificación.

El adjudicatario será responsable de que las herramientas propuestas no presenten vulnerabilidades conocidas en el momento de su puesta en servicio, así como, garantizar su actualización y mantenimiento durante toda la prestación, incorporando su gestión al circuito de incidencias y, en su caso, bloqueando de forma inmediata el acceso cuando resulte necesario.

7.5. D_05 Gestión de activos OT

• Definición del dominio

Conjunto de procesos y procedimientos que el adjudicatario debe implementar para administrar de manera eficiente y segura los activos de OT relacionados con los sistemas IoT del entorno urbano. Esto incluye la clasificación adecuada de cada activo según su función y criticidad, así como la creación y mantenimiento de un inventario centralizado que permita conocer en todo momento el estado y la ubicación de estos activos.

Cuando el adjudicatario sea además fabricante, deberá disponer de su propio inventario interno de los equipos que suministra.

Además, el adjudicatario deberá gestionar de forma rigurosa los procesos de alta, baja y modificación de sus propios activos, asegurando que cualquier cambio quede registrado y autorizado.

- **Cláusulas aplicables**

7.5.1. C_05_01 Clasificación de Activos OT

El adjudicatario deberá entregar, junto con cada dispositivo, sistema o servicio IoT urbano, la información necesaria para su correcta clasificación según criterios de criticidad clínica, nivel de exposición a amenazas, grado de conectividad y cualquier otro dato relevante que facilite la evaluación de riesgos.

La clasificación de activos realizada deberá estar integrada con los mecanismos de gestión de riesgos, permitiendo una evaluación continua y sistemática de las vulnerabilidades asociadas al entorno urbano.

7.5.2. C_05_02 Inventario de Activos

El adjudicatario deberá proporcionar, en el momento de la entrega, los datos técnicos necesarios a la entidad contratante para incorporar los dispositivos y sistemas IoT urbano en el inventario centralizado, incluyendo aspecto como modelo, versión de firmware, fabricante, ubicación física, número de serie y estado operativo.

El inventario centralizado podrá ser creado y gestionado directamente por la entidad contratante, por el adjudicatario o de forma conjunta, según lo determine la entidad en función de sus recursos y capacidades. En todos los casos, el adjudicatario deberá garantizar la correcta integración, actualización y disponibilidad del inventario conforme a los procedimientos establecidos.

Asimismo, cuando el adjudicatario sea además fabricante, deberá mantener su propio inventario interno de los equipos que suministra, asignando un responsable técnico y registrando toda información relevante para su trazabilidad y gestión.

7.5.3. C_05_03 Control de Alta, Baja y Modificación de Activos

El adjudicatario deberá implementar un procedimiento formal y documentado para registrar, comunicar y respaldar cualquier alta, modificación, traslado o baja de los activos IoT urbanos relacionados con los servicios prestados en el marco del presente contrato.

Además, deberá aportar la documentación y datos técnicos necesarios para mantener la trazabilidad completa de los dispositivos y sistemas, así como de los datos tratados por los mismos, asegurando que toda actuación quede adecuadamente registrada y reportada a la entidad contratante.

7.6. D_06 Configuración segura

- **Definición del dominio**

Conjunto de prácticas y procedimientos que el adjudicatario debe seguir para garantizar que todos los dispositivos y sistemas IoT urbanos se configuren inicialmente con los parámetros de seguridad adecuados. Esto incluye aplicar configuraciones predeterminadas seguras que minimicen las vulnerabilidades y reduzcan los riesgos de ataques o fallos.

Además, el adjudicatario debe deshabilitar o restringir los servicios y funciones no necesarias en los dispositivos y sistemas, evitando que componentes sin uso se conviertan en posibles vectores de ataque.

- **Cláusulas aplicables**

7.6.1. C_06_01 Configuración Inicial Segura

El adjudicatario garantizará que, en el momento de la entrega y despliegue de los dispositivos, sistemas y servicios relacionados con IoT en el entorno urbano, sean configurados siguiendo los parámetros de configuración segura definidos por el fabricante y alineados con las buenas prácticas de ciberseguridad, evitando así el uso de configuraciones predeterminadas inseguras.

Paralelamente, todas las credenciales predeterminadas por el fabricante serán cambiadas inmediatamente después de la instalación del dispositivo y antes de su primer uso, garantizando así que no se utilicen credenciales de fábrica.

7.6.2. C_06_02 Deshabilitación de Servicios

El adjudicatario deshabilitará todos los servicios y puertos no necesarios en los dispositivos, sistemas y servicios relacionados con IoT para minimizar la superficie de ataque, asegurando que solo permanezcan funcionales los estrictamente necesarios para el funcionamiento del dispositivo.

7.7. D_07 Actualizaciones de software

- **Definición del dominio**

Conjunto de políticas y procedimientos que el adjudicatario deberá seguir para garantizar la correcta gestión, validación, distribución e instalación de actualizaciones de software en los dispositivos, plataformas o sistemas asociados a soluciones IoT urbanas. Esto incluye definir políticas claras para la gestión de actualizaciones, implementar mecanismos automáticos cuando sea posible y asegurar que las actualizaciones se realicen mediante canales protegidos para evitar riesgos de seguridad.

Asimismo, el adjudicatario deberá evaluar el impacto de cada actualización, realizar pruebas previas que aseguren su correcto funcionamiento y documentar todo el proceso asociado. Además, deberá notificar a la entidad contratante sobre las actualizaciones realizadas para mantener la transparencia y la trazabilidad en la gestión del software.

- **Cláusulas aplicables**

7.7.1. C_07_01 Políticas de Actualización

El adjudicatario deberá establecer y mantener políticas claras y documentadas para la actualización de hardware y software de los dispositivos conectados, garantizando que todos los dispositivos estén equipados con los últimos parches de seguridad y firmware antes de ser puestos en producción.

Se implementará un proceso regular y sistemático de actualización y parcheo para mantener los dispositivos, sistemas y servicios relacionados con IoT en el entorno urbano.

Todas las actualizaciones realizadas se harán empleando fuentes y librerías oficiales del fabricante o recomendadas por este.

7.7.2. C_07_02 Actualizaciones Automáticas

Siempre que sea posible y no represente un riesgo para el funcionamiento o el rendimiento de los dispositivos, sistemas y servicios relacionados con IoT, el adjudicatario habilitará procesos de actualización automáticos. Estos procesos permitirán que los dispositivos se actualicen automáticamente para aplicar parches de seguridad y mejoras.

El adjudicatario garantizará que las actualizaciones automáticas sean configurables permitiendo definir horarios de actualización y así minimizar interrupciones en la operativa de los servicios urbanos.

7.7.3. C_07_03 Mecanismos Seguros de Actualización

El adjudicatario deberá implementar mecanismos seguros para la actualización de software, asegurando la autenticidad e integridad de las actualizaciones mediante un plan periódico.

Asimismo, el adjudicatario deberá asegurar la disponibilidad de mecanismos de reversión segura (del inglés, rollback) que permitan restaurar la configuración o versión anterior del sistema o dispositivo en caso de fallo, incompatibilidad, impacto en la operativa urbana o degradación del servicio tras la actualización. El procedimiento de rollback deberá estar documentado, probado y ser ejecutable sin comprometer la integridad de los datos ni la continuidad asistencial.

7.7.4. C_07_04 Evaluación de Impacto y Pruebas

El adjudicatario llevará a cabo, en sus instalaciones, evaluaciones de impacto exhaustivas con el objetivo de evaluar el efecto de las actualizaciones en el funcionamiento de los dispositivos, sistemas y servicios relacionados con IoT en el entorno urbano, así como la seguridad de los ciudadanos antes de su implementación.

Todos los parches y actualizaciones serán revisados y probados en un entorno de pruebas controlado ubicado en las instalaciones del adjudicatario, siguiendo procedimientos estandarizados que permitan minimizar los riesgos de interrupciones y garantizar la resiliencia de los sistemas antes de su despliegue en los entornos de la entidad contratante.

7.7.5. C_07_05 Documentación y Notificación

El adjudicatario deberá disponer de un registro público de versiones accesible para la entidad contratante, donde se documenten todas las actualizaciones de software y firmware distribuidas en dispositivos IoT relacionados con el objeto del contrato, con detalle de las vulnerabilidades corregidas y la fecha de publicación.

Se notificará e informará al personal TI responsable asignado por la entidad contratante sobre las actualizaciones realizadas y cualquier cambio esperado en el funcionamiento de los dispositivos.

7.8. D_08 Gestión de vulnerabilidades

- **Definición del dominio**

Conjunto de procesos que el adjudicatario deberá establecer para identificar, analizar y gestionar de forma proactiva las vulnerabilidades que afecten a los dispositivos, sistemas y servicios IoT del entorno urbano que se encuentren bajo su responsabilidad. Este proceso incluye la realización periódica de

análisis de vulnerabilidades que permitan detectar posibles fallos o debilidades explotables que comprometan la seguridad. Dichos análisis deberán llevarse a cabo exclusivamente en las instalaciones del adjudicatario, siendo responsabilidad de la entidad contratante la monitorización y gestión de las vulnerabilidades de los dispositivos y sistemas desplegados en sus entornos.

El adjudicatario deberá notificar a la entidad contratante cualquier vulnerabilidad identificada en las pruebas y presentar un plan de corrección que asegure su mitigación. El despliegue inicial de los sistemas deberá realizarse libre de vulnerabilidades conocidas, o si debido a limitaciones técnicas, de certificación o de ciclo de vida, no fuera posible alcanzar dicho estado, el adjudicatario deberá aportar una evaluación documentada de los riesgos y aplicar medidas compensatorias que reduzcan la probabilidad.

- **Cláusulas aplicables**

7.8.1. C_08_01 Proceso de Identificación y Gestión de Vulnerabilidades

El adjudicatario deberá implementar y mantener un proceso continuo y proactivo para la identificación y gestión de vulnerabilidades en sus entornos, a lo largo del ciclo de vida de todos los dispositivos, sistemas y servicios relacionados con IoT en el entorno urbano, que se encuentren bajo su responsabilidad, durante toda la vigencia del contrato.

Este proceso deberá incluir la consulta periódica a bases de datos públicas sobre vulnerabilidades reconocidas internacionalmente, así como la utilización de fuentes de inteligencia de amenazas, tales como informes especializados de ciberseguridad y repositorios de vulnerabilidades.

7.8.2. C_08_02 Análisis Regular de Vulnerabilidades

El adjudicatario deberá realizar análisis de vulnerabilidades periódicos sobre los dispositivos, sistemas y servicios relacionados con IoT objeto del contrato, empleando herramientas avanzadas de escaneo y pruebas de penetración.

Dichos análisis deberán llevarse a cabo exclusivamente en las instalaciones del adjudicatario, siendo responsabilidad de la entidad contratante la monitorización y gestión de las vulnerabilidades de los dispositivos y sistemas desplegados en sus entornos.

El adjudicatario documentará de manera exhaustiva las vulnerabilidades, tanto las ya identificadas como las potenciales, asociadas a cada dispositivo, asegurando una transparencia total durante el proceso de resolución.

7.8.3. C_08_03 Notificación y Plan de Corrección

El adjudicatario notificará periódicamente a la entidad contratante los resultados de los análisis de vulnerabilidades realizados en sus instalaciones, incluyendo un informe detallado con las debilidades detectadas en los dispositivos, sistemas y servicios IoT del entorno urbano.

Asimismo, deberá proponer un plan de corrección que contemple la priorización de dichas vulnerabilidades en función de su criticidad, con el fin de facilitar la adopción de medidas correctoras sobre los activos desplegados en las instalaciones de la entidad contratante.

7.8.4. C_08_04 Implantación inicial libre de vulnerabilidades

Los dispositivos conectados adquiridos deberán estar libres de vulnerabilidades conocidas en el momento de la instalación en los entornos urbanos.

En caso de que, por razones técnicas o legales, no sea posible un despliegue inicial completamente libre de vulnerabilidades conocidas, el adjudicatario deberá proporcionar a la entidad contratante el último informe de análisis de vulnerabilidades disponible. Dicho informe deberá identificar las vulnerabilidades conocidas hasta la fecha, evaluar el nivel de riesgo asociado a cada una y presentar un plan de corrección y priorización que contemple los plazos estimados para su resolución. Asimismo, el adjudicatario deberá proponer e implementar las medidas de seguridad compensatorias necesarias para reducir la probabilidad de explotación de las vulnerabilidades no corregidas, de forma que el riesgo residual se mantenga por debajo del umbral de riesgo aceptable definido por la entidad contratante.

7.9. D_09 Desarrollo seguro

- **Definición del dominio**

Conjunto de prácticas y procesos que el adjudicatario deberá implementar en el diseño, desarrollo, validación y mantenimiento de soluciones IoT del entorno urbano, garantizando así la seguridad desde las primeras fases del ciclo de vida del software (SDLC).

Además, el desarrollo deberá cumplir con la regulación aplicable, con el objetivo de prevenir vulnerabilidades y minimizar de forma proactiva los riesgos de seguridad, en lugar de limitarse únicamente a su corrección tras la aparición de fallos.

- **Cláusulas aplicables**

7.9.1. C_09_01 Seguridad desde el diseño

El adjudicatario deberá garantizar que todos los dispositivos IoT urbanos, así como el software asociado, suministrados en el marco del presente contrato, cuenten, en el momento de su entrega, con:

- Marcado CE válido, colocado en el dispositivo, así como la documentación asociada que acredite que el producto cumple con los requisitos relativos a la seguridad desde el diseño y por defecto establecidos en el Reglamento (UE) 2024/2847 (CRA).
- Declaración UE de Conformidad, expedida por el fabricante, en la que se manifieste, bajo su responsabilidad, que el dispositivo cumple con todos los requisitos aplicables establecidos en la normativa europea vigente. Esta declaración deberá estar disponible para la entidad contratante.
- Documentación técnica actualizada, emitida por el fabricante, que permita verificar el cumplimiento de los requisitos de seguridad, interoperabilidad y ciberseguridad, incluyendo las especificaciones aplicables para su integración en el entorno operativo de la entidad contratante.

Sin la presentación y validación previa de estas certificaciones y documentos, el dispositivo no podrá ser aceptado ni autorizado para su puesta en producción en los entornos de la entidad contratante.

7.10. D_10 Mantenimiento físico de los dispositivos

- **Definición del dominio**

Conjunto de actividades preventivas, correctivas y predictivas necesarias para garantizar la operatividad y buen estado físico de los dispositivos, sistemas y servicios relacionados con IoT durante su ciclo de vida útil. El adjudicatario será responsable de coordinarse con los equipos técnicos y operativos para planificar y ejecutar las tareas de mantenimiento, minimizando los tiempos de inactividad.

- **Cláusulas aplicables**

7.10.1. C_10_01 Coordinación con el equipo técnico y operativo

El adjudicatario deberá establecer mecanismos de coordinación efectiva, continua y documentada con los equipos técnicos y operativos de la entidad contratante para todas las actividades relacionadas con la instalación, configuración, integración, mantenimiento y actualización de los dispositivos, sistemas y servicios relacionados con IoT en el entorno urbano. Esta coordinación será esencial para garantizar la seguridad de los ciudadanos, la interoperabilidad con los sistemas públicos y la operatividad de los servicios urbanos.

También, el adjudicatario deberá designar interlocutores técnicos cualificados que actúen como puntos de contacto con las áreas responsables de la entidad contratante, así como facilitar la planificación conjunta de intervenciones, validaciones funcionales y pruebas de integración. Toda acción que pueda afectar el funcionamiento de los dispositivos conectados o la disponibilidad de los servicios urbanos deberá ser previamente comunicada, acordada y autorizada por la entidad contratante.

7.11. D_11 Acceso de emergencia autorizado al dispositivo

- **Definición del dominio**

Conjunto de procedimientos y mecanismos que permiten el acceso inmediato y controlado a dispositivos IoT en situaciones de emergencia, cuando los métodos habituales de autenticación no son viables y es necesario garantizar la continuidad de los servicios críticos urbanos. Este acceso debe estar debidamente autorizado, registrado y monitoreado para evitar abusos o accesos indebidos.

- **Cláusulas aplicables**

7.11.1. C_11_01 Mecanismo de Acceso de Emergencia

El adjudicatario deberá implementar en los dispositivos, sistemas y servicios relacionados con IoT un mecanismo de acceso de emergencia que permita a los usuarios autorizados acceder temporalmente a funciones críticas del dispositivo en situaciones excepcionales, cuando los controles de acceso estándar puedan impedir la gestión o recuperación rápida del servicio.

El adjudicatario deberá asegurar que el acceso de emergencia solo pueda ser realizado por personal de que esté previamente autorizado por la entidad contratante, técnicamente limitado en su alcance, registrado de forma completa y trazable, y sujeto a revisión posterior. Los mecanismos de acceso de emergencia deben activarse solo bajo condiciones justificadas y conforme a políticas predefinidas, garantizando en todo momento la integridad del sistema y la confidencialidad de los datos.

7.12. D_12 Seguridad contra el código dañino

- **Definición del dominio**

Conjunto de medidas técnicas, organizativas y procedimentales que el adjudicatario deberá implementar para prevenir, detectar y responder contra la infección y propagación de software malicioso en los dispositivos, sistemas y entornos relacionados con IoT. Esto implica el uso de software antivirus actualizado y soluciones especializadas de detección y respuesta ante amenazas para identificar y mitigar riesgos de forma eficaz.

- **Cláusulas aplicables**

7.12.1. C_12_01 Uso de software de protección contra código dañino

Siempre que las especificaciones del fabricante del dispositivo y sus sistemas relacionados lo permitan, se utilizará software para la protección contra código dañino que pudiera comprometer el uso de los dispositivos por parte de actores de amenazas.

Tendrán siempre preferencia los sistemas de protección contra código dañino propios de la entidad contratante, ya que sus alertas son monitorizadas y supervisadas por la propia entidad y/o sus CERT de referencia.

En aquellos casos los que el fabricante del dispositivo imponga una determinada herramienta para la protección contra código dañino, el adjudicatario deberá especificar quién o qué organismo o empresa y de qué forma se monitorizan las alertas ocurridas en los dispositivos objeto de adjudicación, así como de qué forma se comunicarán estas al CERT de referencia de la entidad contratante.

Los productos o servicios de seguridad propuestos por el fabricante deberán figurar en el CPSTIC del CCN-CERT, o, en su defecto, contar con certificaciones equivalentes que acrediten la funcionalidad de seguridad requerida, como el cumplimiento de lo establecido en el artículo 19 del ENS en caso de la prestación de servicios.

Asimismo, para todos los productos o servicios propuestos, el tiempo de comunicación de alertas será siempre inmediato, es decir, en tiempo real.

En todo caso, si el sistema relacionado con el dispositivo presta un servicio web, este deberá ser protegido frente a ataques de manipulación, inyección de código e inyección SQL al menos mediante validación y saneamiento de entradas, uso de funciones seguras, control de accesos y privilegios, filtros y escapes de caracteres especiales, manejo adecuado de errores, etc.

Adicionalmente, la monitorización de la seguridad de los dispositivos en los entornos de la entidad contratante será responsabilidad exclusiva de esta, siguiendo sus propias políticas y procedimientos. El adjudicatario únicamente deberá garantizar que, en el manual de seguridad, se incluyan los mecanismos y recomendaciones de seguridad proporcionados por el fabricante para su correcta integración y gestión.

7.13. D_13 Capacidad de bloqueo del dispositivo

- **Definición del dominio**

Conjunto de medidas técnicas que deberán incorporar los dispositivos, sistemas y servicios relacionados con IoT urbano para permitir, de forma controlada, el bloqueo, desactivación o limitación funcional ante la detección de fallos críticos, condiciones anómalas, riesgos para la seguridad ciudadana o incumplimientos normativos.

El adjudicatario será responsable de garantizar que esta funcionalidad esté prevista desde el diseño, integrando mecanismos para la gestión de riesgos residuales en los dispositivos, incluyendo la posibilidad de suspender su uso si comprometen la seguridad o la prestación de servicios esenciales.

- **Cláusulas aplicables**

7.13.1. C_13_01 Niveles de Bloqueo Configurables

Los dispositivos IoT implementados por parte del adjudicatario deberán permitir la configuración de múltiples niveles de bloqueo según el contexto técnico o administrativo definido por la entidad contratante:

- Bloqueo total (inhabilitación completa del dispositivo).
- Bloqueo funcional (inhabilitación de funciones específicas).
- Bloqueo temporal (suspensión programada o automatizada).

7.14. D_14 Gestión de eventos

- **Definición del dominio**

El adjudicatario deberá implementar un conjunto de procesos y herramientas que garanticen la correcta generación, almacenamiento, y análisis de los registros de seguridad y configuración (logs) en los dispositivos y sistemas IoT del entorno urbano a lo largo de toda su vida útil.

La gestión de eventos por parte del adjudicatario podrá abarcar la detección proactiva de incidencias, mediante el análisis de registros y mecanismos automatizados, o bien, cuando así lo determine expresamente la entidad contratante, centrarse exclusivamente en la recepción, registro, análisis y resolución de las incidencias que le sean notificadas. Los sistemas del adjudicatario deberán permitir la trazabilidad de las acciones críticas y la generación de informes sobre el estado y evolución de dichas incidencias.

- **Cláusulas aplicables**

7.14.1. C_14_01 Registros de Seguridad y Configuración de Logs

Los dispositivos IoT deberán permitir la activación y configuración de registros de seguridad de manera detallada y continua, garantizando la trazabilidad de eventos y acciones críticas durante toda su vida útil.

El adjudicatario deberá disponer de mecanismos adecuados de detección proactiva de incidencias, mediante el análisis de registros y herramientas automatizadas, o bien, cuando así lo determine

expresamente la entidad contratante, contar con sistemas de ticketing u otros mecanismos equivalentes que aseguren la correcta evaluación, priorización y atención de las incidencias derivadas de vulnerabilidades, errores operativos o sospecha de incidentes de seguridad.

La configuración de los dispositivos, sistemas y servicios relacionados con IoT urbano deberá permitir establecer políticas de retención de logs adecuadas para asegurar que los registros estén disponibles en caso de auditoría, durante un período determinado conforme a las mejores prácticas y regulaciones aplicables.

Los registros deberán almacenarse en formatos estructurados y estandarizados, preferentemente XML, JSON o Syslog, que permitan su integración automatizada con herramientas de análisis, sistemas de monitorización urbana o plataformas de seguridad (como SIEM o CMDB). Los formatos seleccionados deberán garantizar la interoperabilidad, la legibilidad técnica y la integridad de los datos registrados.

Asimismo, deberá habilitarse un perfil de auditor con permisos únicamente de lectura, que pueda acceder y visualizar los logs en caso de incidente, facilitando la trazabilidad y el análisis forense sin comprometer la integridad de la información.

7.14.2. C_14_02 Monitorización Continua y Revisión de Auditoría

Los entornos IoT urbanos deberán permitir la monitorización continua mediante sistemas automatizados desplegados por la entidad contratante, o en su caso, por el adjudicatario cuando así se haya definido en el contrato, para la detección de intrusiones, accesos no autorizados, actividades sospechosas o no autorizadas.

Los dispositivos y sus sistemas de información relacionados dispondrán de las capacidades necesarias para que la entidad contratante pueda realizar revisiones periódicas de los registros de auditoría, con el objetivo de identificar cualquier acceso no autorizado o actividad sospechosa.

7.15. D_15 Gestión de incidentes

• Definición del dominio

Conjunto de procesos y procedimientos que el adjudicatario deberá implementar para la detección, notificación, análisis, contención, resolución y documentación de incidentes que afecten a la disponibilidad, integridad, confidencialidad o funcionamiento de los dispositivos, sistemas y servicios relacionados con IoT urbano.

El adjudicatario deberá establecer mecanismos de respuesta rápida y escalado de alertas, así como canales de comunicación efectivos con los equipos operativos y técnicos de la entidad contratante, y reportar a las autoridades competentes cuando la normativa lo requiera.

• Cláusulas aplicables

7.15.1. C_15_01 Proceso Integral de Gestión de Incidentes

El adjudicatario dispondrá de un procedimiento integral para hacer frente a los incidentes ocurridos en los entornos desplegados bajo su responsabilidad o en sus propias instalaciones que puedan tener impacto en la seguridad de los sistemas o servicios que presta a la entidad contratante. Este proceso

incluirá procedimientos claros y detallados para la detección, análisis, contención, erradicación y recuperación de incidentes de seguridad.

Paralelamente, el adjudicatario asignará roles y responsabilidades específicas a miembros del equipo técnico de cara a garantizar una gestión eficaz de los incidentes, incluyendo la capacidad de asignar recursos para detectar, contener, erradicar, recuperar y analizar las consecuencias del incidente.

En caso de incidente de seguridad que afecte a dispositivos, sistemas y servicios relacionados, el adjudicatario deberá garantizar la preservación íntegra de la cadena de custodia de toda la evidencia técnica relevante, con el fin de permitir un análisis forense preciso, la identificación de vectores de ataque y, en su caso, la utilización de dicha evidencia en procedimientos administrativos, regulatorios o judiciales.

El adjudicatario deberá implementar procedimientos formalmente documentados que aseguren la recogida, conservación, transporte, acceso y análisis de evidencias digitales (como imágenes de memoria o disco, registros de acceso, trazas de actividad del sistema, etc.), aplicando técnicas que preserven su autenticidad, integridad y trazabilidad.

7.15.2. C_15_02 Procedimientos de Contención y Recuperación

El adjudicatario implementará procedimientos de contención con la mayor eficacia posible, limitando el alcance y el impacto de los incidentes de seguridad ocurridos en los entornos gestionados o en sus instalaciones que puedan afectar a los dispositivos, sistemas y servicios objeto del contrato.

7.15.3. C_15_03 Notificación de Incidentes

El adjudicatario notificará, sin dilación, a los responsables de la entidad contratante y a las autoridades competentes sobre los incidentes de seguridad ocurridos, según lo requieran las normativas aplicables y cuando el incidente pudiera afectar a los servicios prestados por el adjudicatario a la entidad o este pudiera repercutir de alguna forma en sus dispositivos, sistemas y servicios relacionados con IoT urbano. Asimismo, el adjudicatario informará de las actuaciones llevadas a cabo para la resolución del incidente y su impacto en la operativa.

Se definirán claramente las cadenas de mando y las responsabilidades de comunicación de forma proactiva antes de que sucedan incidentes, con el objeto de asegurar una respuesta coordinada y eficiente entre el adjudicatario y la entidad contratante.

7.15.4. C_15_04 Canales de Comunicación para Incidentes

Para una comunicación ágil de los incidentes, el adjudicatario deberá emplear los canales de comunicación establecidos por la entidad contratante, asegurando que la información llegue a todos los involucrados.

El adjudicatario utilizará estos canales para el reporte y seguimiento de incidentes de seguridad mediante los protocolos de comunicación definidos, garantizando que todas las partes interesadas sean informadas adecuadamente durante un incidente.

Esto incluirá la comunicación con el personal interno de la entidad contratante, otros proveedores, autoridades y usuarios, en su caso.

7.16. D_16 Gestión segura de la cadena de suministro

- **Definición del dominio**

Conjunto de mecanismos y controles que el adjudicatario debe implementar para garantizar la seguridad, integridad y fiabilidad de todos los elementos, actores y procesos que intervienen en la cadena de suministro de los dispositivos, componentes, software, servicios y actualizaciones asociados a los entornos IoT urbanos desplegados.

La gestión segura de la cadena de suministro incluye la evaluación continua de los riesgos asociados a proveedores, subcontratistas y terceros del adjudicatario, la protección contra manipulaciones durante el transporte, almacenamiento o integración, y la aplicación de requisitos de ciberseguridad.

- **Cláusulas aplicables**

7.16.1. C_16_01 Evaluación de Terceros Proveedores relacionados con la adjudicación

El adjudicatario dispondrá de mecanismos y criterios de seguridad rigurosos para la evaluación y selección de sus propios proveedores que tengan relación con la relación contractual. Dichos criterios deben incluir la revisión de las políticas de seguridad, prácticas de manejo de datos, y medidas de ciberseguridad implementadas por los proveedores.

El adjudicatario dispondrá de la capacidad para llevar a cabo auditorías periódicas de seguridad de sus proveedores para asegurar que cumplen con los requisitos de seguridad establecidos. Las auditorías deben incluir evaluaciones de vulnerabilidades, revisiones de cumplimiento normativo y pruebas de penetración. En su defecto podrán exigir las certificaciones de seguridad equivalentes de acuerdo con la normativa aplicable.

7.16.2. C_16_02 Contratos y Acuerdos

El adjudicatario incluirá cláusulas de seguridad específicas en todos los contratos y acuerdos con sus proveedores relacionados con esta adjudicación. Estas cláusulas deben cubrir aspectos como la protección de datos, la respuesta a incidentes, la gestión de acceso y la obligación de mantener actualizadas las medidas de seguridad.

Estos contratos se revisarán periódicamente para asegurar que las cláusulas de seguridad sigan siendo relevantes y efectivas. Las revisiones deben tener en cuenta cambios en las normativas, avances tecnológicos y lecciones aprendidas de incidentes de seguridad pasados.

Es de mencionar, que todas las cláusulas de seguridad de la información y ciberseguridad desarrolladas en el presente pliego, en el caso de disponer de terceros que realicen alguna operación sobre los dispositivos, sistemas y servicios relacionados con IoT en el entorno urbano, serán de aplicación directa, siendo el adjudicatario responsable de su traslado y cumplimiento.

7.17. D_17 Gestión de la obsolescencia

- **Definición del dominio**

Conjunto de procesos y estrategias que el adjudicatario debe aplicar para anticipar, identificar, mitigar y gestionar los riesgos asociados a la obsolescencia tecnológica, funcional o normativa de dispositivos, componentes, software y servicios vinculados a soluciones IoT urbanas.

El adjudicatario debe establecer un plan de restitución y transferencia tecnológica que contemple tiempos, recursos y coordinación con la entidad contratante, garantizando una transición ordenada y sin interrupciones en los servicios asociados.

- **Cláusulas aplicables**

7.17.1. C_17_01 Planificación de la Restitución y Transferencia Tecnológica

El adjudicatario presentará una planificación detallada para la restitución y transferencia tecnológica, contemplando medios, acciones de contingencia y riesgos potenciales.

Cuando sea necesario, se incluirá un período de transición para la gestión organizada del proceso de transferencia. En este sentido, el adjudicatario elaborará un plan detallado de transición que incluya todas las etapas del proceso, asegurando la coordinación efectiva entre todas las partes involucradas.

7.18. D_18 Protección de los servicios Cloud

- **Definición del dominio**

Conjunto de medidas técnicas, organizativas y contractuales que el adjudicatario debe implementar para garantizar la seguridad y privacidad de los datos personales almacenados y procesados en servicios cloud relacionados con el objeto del contrato. Esto incluye informar y documentar claramente donde se almacenan y procesan los datos personales, asegurando que se apliquen las medidas adecuadas para protegerlos frente a accesos no autorizados, pérdidas o filtraciones, respetando siempre la legislación vigente sobre protección de datos.

- **Cláusulas aplicables**

7.18.1. C_18_01 Localización y Ubicación Geográfica de los Datos Personales

El adjudicatario deberá informar a la entidad contratante sobre la ubicación geográfica de los datos, incluidas copias de seguridad y almacenamiento de logs, antes y durante el suministro del servicio.

Si los dispositivos IoT o sus sistemas relacionados manejan datos personales ubicados en la nube, se deberá asegurar en todo momento que la localización de los servidores donde se almacenan estos datos se encuentre en territorio de la Unión Europea, o, en su caso, en países o entidades que ofrezcan garantías adecuadas conforme al RGPD, mediante decisiones de adecuación la Comisión Europea o la aplicación de cláusulas contractuales. Asimismo, cualquier cambio de ubicación deberá de ser notificado y aprobado por la entidad contratante.

Con respecto a los datos almacenados, se deberá cumplir con la Ley 3/2018 (

LOPDGDD y el resto de las normativas relacionadas en materia de protección de datos, junto a los perfiles de cumplimiento en ciberseguridad establecidos por el ENS (CCN-STIC 823) y estándares, como la ISO 27001 e ISO 27017.

El adjudicatario deberá colaborar en todo momento con el responsable del tratamiento designado por la entidad contratante de cara a garantizar el ejercicio de los derechos de protección de datos conforme a las normativas aplicables.

7.19. D_19 Continuidad de negocio

• Definición del dominio

Conjunto de políticas y procedimientos que el adjudicatario deberá establecer para garantizar la continuidad operativa de los dispositivos, sistemas y servicios IoT urbanos objeto del contrato en situaciones de interrupción, fallo crítico, desastre tecnológico o contingencia externa. Estas medidas deberán asegurar la integridad de los datos, minimizar el impacto en la prestación de los servicios afectados y permitir el restablecimiento de la operatividad en plazos definidos y aceptables.

Asimismo, el adjudicatario deberá proporcionar a la entidad contratante la documentación técnica, las recomendaciones y el soporte necesarios para facilitar la integración de dichos dispositivos y sistemas en los planes de continuidad de negocio de la entidad. Esta coordinación permitirá a la entidad contratante definir, actualizar y ejecutar sus propios planes de respaldo, recuperación y contingencia, contando con la información y soporte adecuados por parte del adjudicatario.

• Cláusulas aplicables

7.19.1. C_19_01 Procedimientos de Respaldo y Recuperación

El adjudicatario deberá establecer y documentar políticas y procedimientos que garanticen la continuidad operativa de los dispositivos, sistemas y servicios IoT urbanos objeto del contrato en situaciones de interrupción, fallo crítico, desastre tecnológico o contingencia externa. Dichos procedimientos deberán asegurar la integridad de los datos, minimizar el impacto en la prestación de los servicios afectados y permitir el restablecimiento de la operatividad en plazos definidos y aceptables.

Además, el adjudicatario deberá proporcionar, junto con la documentación técnica de los dispositivos, sistemas y servicios IoT, los procedimientos recomendados para la realización de copias de seguridad, restauración controlada y recuperación de la información almacenada o gestionada por los equipos suministrados. Estos procedimientos deberán incluir como mínimo:

- Recomendaciones sobre la periodicidad de las copias de seguridad.
- Procedimientos de restauración verificados y probados sobre los dispositivos.
- Recomendaciones sobre cifrado y almacenamiento seguro de la información crítica.

7.19.2. C_19_02 Plan de Recuperación ante Contingencias

El adjudicatario deberá aportar la información técnica necesaria para que la entidad contratante pueda incluir los dispositivos y sistemas IoT urbanos en su plan de recuperación ante contingencias. La responsabilidad de ejecutar o coordinar dicho plan sobre la infraestructura de la entidad corresponderá

a la entidad contratante, salvo que en el contrato establezca expresamente que dichas tareas deban ser asumidas por el adjudicatario.

En los casos en que el contrato incluya servicios gestionados relacionados con IoT urbano, los niveles de servicio, tiempos máximos de respuesta y procedimientos de recuperación estarán definidos mediante los Acuerdos de Nivel de Servicio (ANS) acordados entre las partes.

7.20. D_20 Auditorías técnicas y de cumplimiento

• Definición del dominio

Conjunto de procesos relacionados con la realización o facilitación, de auditorías técnicas y/o de cumplimiento sobre las plataformas, servicios y actividades relacionadas con dispositivos, sistemas y servicios IoT urbanos, tanto antes como después del despliegue. Estas auditorías permiten a la entidad contratante verificar la conformidad con los requisitos técnicos, normativos, contractuales y de seguridad establecidos, así como con la normativa vigente.

El adjudicatario deberá contar con la capacidad técnica y los recursos necesarios para llevar a cabo estas pruebas y auditorías previas al despliegue, documentar sus resultados y ejecutar acciones correctivas cuando se detecten desviaciones o vulnerabilidades.

• Cláusulas aplicables

7.20.1. C_20_01 Requisitos de Pruebas de Seguridad

El adjudicatario deberá garantizar la realización de pruebas de seguridad sistemáticas y documentadas sobre todos los dispositivos, sistemas y servicios relacionados con IoT urbano previas a su puesta en producción, con el fin de identificar vulnerabilidades técnicas, errores de configuración, riesgos de exposición de datos y posibles vectores de ataque que puedan comprometer la confidencialidad, integridad, disponibilidad o trazabilidad de la información y de la operativa urbana.

Las pruebas deberán realizarse en coordinación con el órgano responsable de ciberseguridad de la entidad contratante, que tendrá la autoridad para suspender temporalmente el despliegue en caso de detectarse vulnerabilidades que puedan comprometer la seguridad de la entidad.

7.20.2. C_20_02 Capacidad para Pruebas de Seguridad y Auditorías

Los dispositivos, sistemas y servicios relacionados con IoT urbano adquiridos deberán tener la capacidad de ser sometidos a pruebas de seguridad y auditorías que verifiquen al menos los siguientes aspectos:

- Auditorías de seguridad sobre el registro de actividades de los dispositivos y los sistemas de información relacionados.
- Revisiones de auditoría para identificar accesos no autorizados o actividades sospechosas, incluyendo la monitorización en tiempo real mediante herramientas automatizadas y el envío de telemetría a herramientas de correlación de datos.
- Revisión y evaluación del cumplimiento y la efectividad de las políticas de seguridad de la entidad contratante, incluyendo la necesidad de ajustes según sea necesario.
- Revisión y evaluación del cumplimiento normativo para asegurar el alineamiento con normativas y estándares relevantes.

- Evaluación de los controles técnicos y los procedimientos de seguridad del proveedor.

El adjudicatario deberá colaborar, cuando sea requerido, con la entidad contratante en la realización de auditorías y pruebas de seguridad periódicas sobre los dispositivos, sistemas y servicios relacionados con IoT urbano, ya sea tras cambios significativos en los mismos o ante la sospecha de incidentes de seguridad. Esta colaboración tiene por objeto asegurar el cumplimiento de las políticas de seguridad, facilitar la detección de vulnerabilidades y posibles brechas, y contribuir a la evaluación de la resiliencia de los dispositivos frente a posibles ataques.

Todas las auditorías y pruebas de seguridad de los dispositivos en entornos productivos serán gestionadas exclusivamente por la entidad contratante, ya sea directamente o mediante la contratación de auditores externos, salvo que en el contrato establezca expresamente que dichas tareas deban ser asumidas por el adjudicatario.

Asimismo, la entidad contratante se reserva el derecho de llevar a cabo auditorías de cumplimiento sobre los servicios prestados por el adjudicatario para garantizar que dichas tecnologías se ajustan a los requisitos legales, técnicos y normativos aplicables en el entorno urbano.

7.20.3. C_20_03 Pruebas de Validación Post-Despliegue

El adjudicatario deberá realizar, en caso de ser requerido y siempre bajo la supervisión y validación de la entidad contratante, pruebas de validación posteriores al despliegue para todos los dispositivos IoT urbanos y sistemas asociados que sean instalados, configurados o actualizados en el marco del presente contrato.

Estas pruebas tendrán como objetivo verificar la correcta operatividad funcional, garantizar la integración segura con la infraestructura urbana, evaluar la estabilidad del sistema y confirmar la ausencia de vulnerabilidades o fallos de configuración que puedan generar interferencias o impactos no deseados en los servicios.

7.21. D_21 Formación y concienciación en ciberseguridad

• Definición del dominio

Conjunto de programas y actividades que el adjudicatario deberá implementar para capacitar y sensibilizar a todo el personal involucrado en el diseño, mantenimiento y soporte de dispositivos, sistemas y servicios IoT urbanos sobre las mejores prácticas de seguridad. Estos programas deberán incluir un plan formativo y de concienciación en materia de ciberseguridad actualizado y adecuado en relación con los riesgos específicos en materia de ciberseguridad en el entorno urbano.

• Cláusulas aplicables

7.21.1. C_21_01 Programas de Formación

El adjudicatario contará con programas de formación en ciberseguridad para todos sus empleados implicados con alguno de los siguientes aspectos: diseño, soporte o mantenimiento de dispositivos, sistemas y servicios relacionados con IoT urbano.

La formación deberá cubrir los fundamentos de la ciberseguridad, la protección de datos, el reconocimiento de amenazas comunes y las políticas de seguridad de la organización.

Los programas ofrecerán una formación continua y actualizaciones periódicas sobre nuevas amenazas y mejores prácticas de seguridad.

7.21.2. C_21_02 Concienciación de Seguridad

De igual forma, el adjudicatario mantendrá campañas de concienciación regulares para todos los empleados, incluyendo aquellos implicados en el diseño, soporte o mantenimiento de soluciones IoT urbanas con la finalidad de reducir el riesgo humano como vector de ataque en entornos urbanos y tecnológicos sensibles.

Dicha concienciación deberá incluir contenidos prácticos sobre identificación y prevención de ataques de phishing, suplantación de identidad, ingeniería social, manipulación de correos electrónicos, uso indebido de dispositivos móviles o USB, navegación segura, y riesgos derivados de accesos remotos inseguros o credenciales compartidas.

Análogamente, se fomentará además el reporte inmediato de incidentes sospechosos, errores operativos o accesos no autorizados.

7.22. D_22 Protección física de los dispositivos

- **Definición del dominio**

Conjunto de medidas y controles que se deberán implementar para asegurar la integridad, disponibilidad y seguridad física de los dispositivos IoT urbanos frente a accesos no autorizados, manipulaciones indebidas, robos, sabotajes, daños accidentales o condiciones ambientales adversas. Estas medidas incluyen el control de acceso a las instalaciones, protección ambiental y el uso de elementos físicos de seguridad adecuados.

- **Cláusulas aplicables**

7.22.1. C_22_01 Protección Física de los Dispositivos

Cuando el adjudicatario actúe como fabricante del dispositivo, deberá establecer las medidas de protección física de los dispositivos IoT urbanos, de acuerdo con la criticidad del procesamiento de datos y el entorno de operación. El conjunto de medidas de protección deberá cumplir con la regulación aplicable en materia de protección de instalaciones e infraestructuras.

Asimismo, en el caso de implementar dispositivos IoT urbanos, el adjudicatario deberá informar a la entidad contratante sobre las directrices del fabricante, garantizando que los dispositivos objeto del contrato estén protegidos contra manipulaciones no autorizadas.

Paralelamente, el adjudicatario deberá colaborar con el personal técnico y de seguridad de la entidad contratante, si es requerido, en la implementación de políticas y procedimientos físicos de control de accesos a salas técnicas, armarios de red, zonas técnicas u otras ubicaciones donde se encuentren operativos los dispositivos, sistemas y servicios relacionados.

7.23. D_23 Comunicaciones seguras

- **Definición del dominio**

Conjunto de medidas y configuraciones técnicas que el adjudicatario deberá implementar para proteger las comunicaciones entre dispositivos IoT, plataformas urbanas, aplicaciones móviles y sistemas externos asegurando la confidencialidad, integridad y disponibilidad de la información transmitida. Esto incluye la correcta configuración y gestión de firewalls, la segmentación de redes para aislar los sistemas críticos y el uso de protocolos seguros que prevengan accesos no autorizados y ataques externos.

- **Cláusulas aplicables**

7.23.1. C_23_01 Configuración de Redes y Comunicaciones

El adjudicatario deberá garantizar que todos los dispositivos, sistemas y servicios relacionados con IoT urbano integrados, desplegados o gestionados en el marco del presente contrato estén protegidos mediante la configuración adecuada de firewalls, tanto a nivel perimetral como local, con el fin de controlar, limitar y monitorizar el tráfico de red intercambiado entre los dispositivos, sistemas y servicios relacionados en el marco del presente contrato con otros sistemas, plataformas o servicios externos, garantizando la confidencialidad, integridad y disponibilidad de la información transmitida.

La configuración de los firewalls deberá estar basada en el principio de mínimo privilegio y limitar el tráfico únicamente a los puertos, protocolos y direcciones estrictamente necesarios para el funcionamiento legítimo de los dispositivos. Quedará expresamente prohibida la exposición innecesaria a redes públicas o la apertura de servicios no documentados, sin la autorización previa y por escrito de la entidad contratante.

Asimismo, el adjudicatario deberá asegurar que los firewalls registren los logs de tráfico relevantes y permitan su integración con plataformas de monitorización o análisis de eventos (SIEM), para facilitar la trazabilidad y detección de posibles accesos no autorizados.

Además, deberá notificar a la entidad contratante cualquier actualización o modificación en la configuración de los firewalls o del entorno operativo que pueda afectar a la arquitectura, infraestructura o funcionalidad del entorno urbano desplegado.

7.24. D_24 Segmentación de la red urbana desplegada

- **Definición del dominio**

Conjunto de directrices y requisitos que el adjudicatario deberá seguir diseñar e implementar una segmentación de red adecuada en los entornos urbanos desplegados. La segmentación deberá aislar dispositivos IoT y servicios relacionados en zonas específicas según su criticidad y función, limitar la propagación de amenazas, controlar los flujos de comunicación entre segmentos mediante listas blancas y proteger los servicios expuestos mediante zonas intermedias (por ejemplo, DMZ) y pasarelas autorizadas. Estas directrices se alinearán con los principios del Esquema Nacional de Seguridad (ENS), la arquitectura de protección de perímetro tipo 6 (APP-6) de las guías CCN-STIC aplicables, y las recomendaciones de seguridad del fabricante.

- **Cláusulas aplicables**

7.24.1. C_24_01 Segmentación por criticidad y función

El adjudicatario deberá elaborar y entregar una propuesta de segmentación de red que clasifique los dispositivos, sistemas y servicios IoT urbanos en zonas diferenciadas. Esta clasificación deberá basarse en criterios como el nivel de criticidad del servicio y su exposición a amenazas, la función que desempeñan los distintos componentes (sensores, actuadores, pasarelas, plataformas de gestión, servicios web, almacenamiento o registros), así como los requisitos de conectividad estrictamente necesarios, incluyendo puertos, protocolos y destinos autorizados.

La segmentación deberá asegurar la separación entre la red corporativa IT, los segmentos OT/IoT urbanos y las zonas intermedias destinadas a servicios expuestos o integraciones externas, incorporando los controles de acceso necesarios. Asimismo, se deberán habilitar pasarelas seguras, autenticadores y mecanismos de autorización que aseguren la interconexión controlada de los segmentos, conforme a la arquitectura APP-6 (CCN STIC 811) y a las recomendaciones del fabricante.

En aquellos casos en que las tecnologías específicas de IoT urbano (como LoRaWAN, NB-IoT o redes celulares) requieran arquitecturas alternativas, podrán aplicarse mecanismos de seguridad equivalentes, siempre que proporcionen un nivel de protección comparable al de APP-6.

Dicha propuesta será revisada y validada por la entidad contratante antes de su despliegue, reservándose esta la facultad de solicitar las modificaciones que considere necesarias para asegurar la adecuación a su política interna de seguridad y a su arquitectura de red.

7.24.2. C_24_02 Comunicaciones seguras y servicios expuestos

El adjudicatario deberá configurar y mantener mecanismos de control de comunicaciones que restrinjan el tráfico a lo estrictamente necesario, aplicando el principio de mínimo privilegio y prohibiendo el uso de protocolos inseguros como FTP, HTTP o TELNET. En este sentido, todas las comunicaciones externas deberán realizarse mediante canales cifrados y autenticados, empleando protocolos seguros como HTTPS/TLS 1.3 o superior.

Cuando existan servicios que requieran exposición a Internet o integración con terceros, estos deberán desplegarse en segmentos específicos con protección reforzada, como zonas desmilitarizadas (DMZ), incorporando autenticación robusta, cifrado de extremo a extremo y políticas de acceso previamente acordadas con la entidad contratante.

La operación y monitorización de la segmentación corresponderán a la entidad contratante, salvo en aquellos casos en que el contrato establezca expresamente servicios gestionados a cargo del adjudicatario.

7.24.3. C_24_03 Protección de segmentos inalámbricos y redes municipales

El adjudicatario deberá implementar controles de seguridad específicos para los segmentos inalámbricos, como las redes Wi-Fi municipales y las redes específicas de sensorización urbana. Entre otros, deberá garantizar la separación de segmentos específicos para dispositivos IoT, aplicar cifrado y autenticación robusta en el acceso inalámbrico, restringir el tráfico únicamente a destinos previamente identificados y autorizados, y asegurar en todo momento la interoperabilidad con la plataforma de gestión urbana y con los sistemas expresamente autorizados.

7.25. D_25 Protección de la información

- **Definición del dominio**

Conjunto de obligaciones y medidas que el adjudicatario deberá aplicar para garantizar la protección de la privacidad de los datos personales tratados en el marco de los dispositivos, sistemas y servicios relacionados con IoT urbano.

Estas medidas implican asegurar que cualquier tratamiento de información por parte del adjudicatario, incluido el acceso durante actividades de soporte, mantenimiento, integración o monitorización, se realice con estricto respeto a los principios de licitud, minimización, limitación de la finalidad, exactitud, confidencialidad e integridad, conforme a lo establecido en el RGPD y la Ley Orgánica 3/2018 LOPDGDD.

- **Cláusulas aplicables**

7.25.1. C_25_01 Medidas de Seguridad para la Protección de Datos

El adjudicatario deberá aplicar las medidas técnicas y organizativas apropiadas para impedir accesos no autorizados, evitar filtraciones o usos indebidos de datos personales, garantizar la trazabilidad de las operaciones sobre información sensible y, colaborar con la entidad contratante en el cumplimiento de los derechos de los interesados, la gestión de brechas de seguridad y la realización de evaluaciones de impacto en la protección de datos cuando así se requiera.

Los dispositivos, sistemas y servicios relacionados con IoT urbano deberán estar en disposición de asegurar el cumplimiento con las regulaciones de protección de datos como el RGPD y la Ley 3/2018 LOPDGDD que protegen la privacidad de los datos de los ciudadanos y la confidencialidad de los datos sensibles. En particular, en aquellos casos que se considere necesario, debido a la sensibilidad de la información tratada por los dispositivos, o en sistemas categorizados en categoría ALTA de acuerdo con el ANEXO I “Categorías de seguridad de los sistemas de información” del ENS, deberán disponer de la capacidad para el cifrado de datos en tránsito y en reposo, utilizando mecanismos de cifrado robustos y autorizados por el Centro Criptológico Nacional (en adelante, CCN), asegurando la confidencialidad de la información.

7.26. D_26 Interoperabilidad segura con microservicios

- **Definición del dominio**

Conjunto de medidas que el adjudicatario debe aplicar para garantizar que la comunicación y el intercambio de información entre microservicios en entornos IoT urbanos se realice de forma segura y controlada. Esto incluye la configuración segura de APIs para proteger los datos transmitidos, prevenir accesos no autorizados y asegurar la integridad y confidencialidad de las comunicaciones.

- **Cláusulas aplicables**

7.26.1. C_26_01 Configuración segura de APIs

En los casos en que los dispositivos suministrados o el desarrollo del servicio por parte del adjudicatario requieran el uso o creación de APIs para la comunicación con otros microservicios, se deberán implementar las siguientes medidas de seguridad:

- Se deberán emplear mecanismos seguros de autenticación, como JSON Web Tokens (JWT) o API Keys.
- Cada suscripción o integración con la API deberá contar con un Client_id y Client_secret únicos. Estos valores deberán mantenerse confidenciales y nunca deben incluirse en código fuente accesible públicamente ni en aplicaciones desplegadas.
- Toda interacción con la API deberá realizarse a través del protocolo HTTPS, utilizando TLS en su versión 1.3 o superior.
- Implementar controles de tasa para limitar el número de solicitudes y mitigar posibles ataques de fuerza bruta o abuso de servicio.
- Los mensajes de error deberán evitar la exposición de información sensible del sistema, limitándose a comunicar lo estrictamente necesario.

7.27. D_27 Protección de los soportes de información

- **Definición del dominio**

Conjunto de mecanismos y procedimientos que el adjudicatario deberá aplicar para garantizar la seguridad, confidencialidad, integridad y disponibilidad de los soportes físicos y digitales que contienen información personal generada, tratada o gestionada por dispositivos, sistemas y servicios relacionados con el objeto del contrato. Esto incluye la correcta devolución, eliminación o destrucción de datos e información al término de la prestación o cuando así se requiera, asegurando que la información sensible no quede accesible o expuesta.

- **Cláusulas aplicables**

7.27.1. C_27_01 Devolución y Destrucción de Datos

El adjudicatario, en el caso de llevar a cabo tratamiento de datos personales durante la prestación de los servicios, deberá disponer de mecanismos que regulen la devolución de la información en el formato de datos y los plazos especificados, o en su defecto, la destrucción de los mismos, proporcionando evidencias certificadas de la realización. Además, deberá seguir un protocolo estandarizado para la devolución y destrucción de datos que incluya pasos detallados y verificables.

Asimismo, el adjudicatario o terceros en el caso de proceder a destruir un soporte o cualquier otro elemento relacionado con un sistema de información deberá de disponer de un certificado de destrucción o borrado seguro emitido por una entidad acreditada garantiza la trazabilidad y conformidad legal del proceso, asegurando que la información sensible ha sido eliminada de forma irreversible y conforme a los estándares de protección de datos.

7.28. D_28 Integración segura con aplicaciones móviles

- **Definición del dominio**

Conjunto de requisitos y controles que el adjudicatario debe aplicar al integrar dispositivos, plataformas o servicios asociados a IoT urbano con aplicaciones móviles utilizadas por ciudadanos, operadores de servicios urbanos o personal técnico.

En caso de que existan aplicaciones móviles asociadas, el adjudicatario será responsable de implementar medidas para limitar los permisos a aquellos estrictamente necesarios para su funcionamiento, evitando accesos innecesarios a funcionalidades o información del dispositivo móvil. Asimismo, deberá restringir su distribución exclusivamente a canales autorizados, impidiendo su publicación o descarga desde markets no autorizados por la entidad contratante.

- **Cláusulas aplicables**

7.28.1. C_28_01 Permisos y funcionalidades limitadas

El adjudicatario deberá garantizar que todas las aplicaciones móviles que estén sincronizadas, vinculadas o integradas con dispositivos IoT urbanos se desarrollen, configuren y puedan operarse con una política de permisos mínimos y funcionalidades estrictamente limitadas al uso operativo o técnico necesario, conforme a los principios de seguridad desde el diseño y por defecto.

Las aplicaciones móviles no deberán solicitar, acceder ni procesar más información o funciones del dispositivo móvil de lo estrictamente imprescindible. Queda expresamente prohibido el uso de permisos excesivos o no justificados, tales como el acceso continuo al micrófono, cámara, ubicación, sensores del dispositivo móvil, o la recopilación de información biométrica, salvo que esté debidamente justificado, documentado, autorizado por la entidad contratante y alineado con el consentimiento del usuario en los casos en que sea requerido.

También, el adjudicatario deberá asegurar que estas aplicaciones incorporen mecanismos seguros de autenticación, cifrado de comunicaciones, control de sesiones activas, y registro de acciones (logs), así como medidas para evitar la manipulación, ejecución de código no autorizado o el acceso no controlado a la información personal o funcional. Cualquier funcionalidad de sincronización con el dispositivo IoT deberá estar limitada, trazada y validada, y no podrá alterar parámetros críticos de funcionamiento del dispositivo salvo que esté autorizado expresamente por la entidad contratante.

La entidad contratante se reserva el derecho de auditar las funcionalidades de las aplicaciones móviles y sus permisos en cualquier momento, así como de exigir su modificación o desactivación si se detectan desviaciones respecto a los principios aquí establecidos.

7.28.2. C_28_02 Restricción de distribución de la aplicación en markets no autorizados

El adjudicatario se compromete a garantizar que las aplicaciones móviles asociadas a los dispositivos IoT urbanos únicamente estén disponibles en tiendas oficiales y autorizadas por la entidad contratante, salvo que se acuerde expresamente otro canal controlado como, por ejemplo, distribución empresarial o MDM.

Queda estrictamente prohibida la publicación, distribución o disponibilidad de dichas aplicaciones en markets no autorizados, alternativos o de terceros que no garanticen el cumplimiento de estándares de seguridad, privacidad y control de versiones.

7.29. D_29 Integración con los Centro de Control Urbano o Plataforma Ciudad Inteligente

- **Definición del dominio**

Conjunto de requisitos, procesos y mecanismos técnicos que el adjudicatario deberá implementar para garantizar la correcta integración de los dispositivos, sistemas y servicios IoT urbanos objeto del contrato con los Centros de Control Urbano (CCU) o la Plataforma Ciudad Inteligente (PCI) de la entidad contratante. Esta integración deberá asegurar el intercambio seguro, eficiente y estandarizado de datos e información, así como la interoperabilidad de los sistemas, garantizando la continuidad operativa y el cumplimiento de los requisitos técnicos y normativos aplicables.

- **Cláusulas aplicables**

7.29.1. C_29_01 Interfaces e interoperabilidad

El adjudicatario deberá garantizar que los dispositivos, sistemas y servicios IoT urbanos incorporen interfaces técnicas, APIs y protocolos necesarios para su integración plena con los Centros de Control Urbano o la Plataforma Ciudad Inteligente de la entidad contratante.

Las interfaces deberán cumplir estándares de interoperabilidad reconocidos tales como OGC SensorThings API, MQTT, RESTful APIs u OPC-UA, así como los protocolos definidos por la entidad contratante.

Asimismo, deberá entregar documentación técnica completa, incluyendo especificaciones, esquemas de datos, formatos soportados y diagramas de arquitectura, así como manuales de operación y procedimientos de integración.

7.29.2. C_29_02 Seguridad en la integración

Todas las comunicaciones entre los dispositivos y sistemas IoT urbanos con la Plataforma Ciudad Inteligente deberán garantizar la confidencialidad, integridad y autenticidad de los datos utilizando mecanismos de cifrado robustos y autorizados por el Centro Criptológico Nacional (CCN).

El adjudicatario deberá implementar mecanismos de autenticación y autorización que cumplan los estándares aplicables, incluyendo el control granular de acceso a datos y servicios.

Además, se deberá registrar y auditar cualquier intercambio de información relevante, asegurando trazabilidad completa.

7.29.3. C_29_03 Monitorización y gestión centralizada

El adjudicatario deberá habilitar capacidades de monitorización remota, control y gestión centralizada de los dispositivos y sistemas IoT urbanos integrados, permitiendo la visualización en tiempo real del estado operativo, indicadores clave y eventos relevantes. Asimismo, deberá garantizar la generación de alertas y notificaciones automáticas hacia la Plataforma Ciudad Inteligente ante incidencias críticas.

Además, el adjudicatario deberá definir procedimientos claros para la actualización y mantenimiento de interfaces y sistemas, asegurando su compatibilidad continua con la plataforma, así como proporcionar soporte técnico especializado durante la fase de integración y operación, incluyendo asistencia ante incidencias o problemas de interoperabilidad.

7.30. D_30 Tratamiento de la información

- **Definición del dominio**

Conjunto de obligaciones que el adjudicatario deberá cumplir para garantizar la correcta transferencia de la documentación, configuraciones, registros y demás información relevante relacionada con los dispositivos, sistemas y servicios IoT urbanos al finalizar el contrato.

Esta transferencia deberá asegurar la continuidad operativa, permitir la trazabilidad de las actuaciones realizadas y facilitar la asignación de responsabilidades por parte de un nuevo adjudicatario o del personal propio de la entidad contratante. Toda la información deberá entregarse en formatos accesibles, estructurados y debidamente documentados, cumpliendo con lo establecido en el RGPD, la Ley Orgánica 3/2018 (LOPDGDD), el Esquema Nacional de Seguridad (ENS), así como con estándares como la ISO/IEC 27001, la ISO 27799 y la IEC 80001.

- **Cláusulas aplicables**

7.30.1. C_30_01 Transferencia de Conocimiento e Información al Finalizar el Contrato

Al término del contrato, ya sea por cumplimiento del plazo de vigencia, rescisión anticipada o cualquier otra causa, el adjudicatario estará obligado a llevar a cabo una transferencia ordenada, completa y documentada del conocimiento, la información técnica y los activos digitales relacionados con los dispositivos, plataformas o servicios IoT urbanos que hayan sido suministrados, mantenidos o gestionados durante la vigencia contractual.

Esta transferencia incluirá, como mínimo, toda la documentación técnica actualizada (manuales, configuraciones, claves de administración si procede, topologías, inventario de dispositivos, informes de mantenimiento y seguridad), registros de eventos e incidentes, credenciales bajo control seguro, logs, licencias, esquemas de integración, así como cualquier conocimiento tácito o explícito necesario para garantizar la continuidad operativa, la seguridad funcional y la posibilidad de asumir la gestión por parte de la entidad contratante o de un nuevo proveedor. La entrega deberá realizarse en formatos estructurados, legibles, verificables y sin restricciones tecnológicas o contractuales que impidan su reutilización.

Asimismo, el adjudicatario se compromete a garantizar que toda la información generada o gestionada en el marco del contrato, incluyendo aquella compartida con terceros subcontratados o proveedores externos, esté debidamente clasificada, protegida y tratada conforme a su nivel de sensibilidad. Cualquier acuerdo suscrito entre el adjudicatario y terceros que implique el acceso, tratamiento o custodia de dicha información deberá incluir cláusulas explícitas que aseguren la clasificación, confidencialidad, integridad y trazabilidad de la misma, alineadas con las políticas de seguridad de la entidad contratante, el ENS, el RGPD, y estándares como ISO/IEC 27001 o ISO 27701.

8. Anexos

Este apartado incluye información complementaria que respalda y amplía el contenido principal del documento.

8.1. Anexo I: Guía para la clasificación de la criticidad de dispositivos y sistemas IoT

El presente anexo tiene por objeto establecer un procedimiento claro, estructurado y comprensible que permita determinar el nivel de criticidad de los dispositivos y sistemas IoT objeto del contrato, conforme a lo establecido en el Esquema Nacional de Seguridad (ENS), aplicando el modelo CIDAT.

Dicha clasificación se realizará conforme a lo establecido en el Esquema Nacional de Seguridad (ENS), aplicando el modelo CIDAT y permitirá identificar qué cláusulas de seguridad deben incorporarse en los pliegos según la tabla de aplicabilidad recogida en el Anexo II.

8.1.1. Introducción al modelo CIDAT

El ENS establece que la seguridad de un sistema debe analizarse considerando cinco dimensiones, conocidas como bajo el acrónimo de CIDAT:

- **Confidencialidad:** ¿La información que maneja el dispositivo debe mantenerse reservada y accesible sólo a quien corresponda?
- **Integridad:** ¿Es crítico que los datos no se alteren o manipulen?
- **Disponibilidad:** ¿Es necesario que el servicio o dispositivo esté siempre accesible y funcionando?
- **Autenticidad:** ¿Es importante asegurar que los datos proceden de una fuente legítima y fiable?
- **Trazabilidad:** ¿Es necesario poder registrar quién, cuándo y cómo accede o modifica la información?

Cada una de estas dimensiones ayuda a valorar el impacto que tendría un incidente sobre el servicio. La combinación de todas ellas permitirá obtener una valoración integral de la criticidad, orientando las medidas de protección a aplicar en cada caso.

8.1.2. Procedimiento para la clasificación

El proceso de clasificación de la criticidad se realizará de acuerdo con los siguientes pasos:

- **Paso 1 – Identificación del dispositivo o sistema IoT**

Defina el dispositivo o sistema IoT a licitar: ¿qué función desempeña?, ¿en qué ubicación estará desplegado?, ¿qué servicio concreto soporta? y ¿de qué otros elementos o sistemas depende?

- **Paso 2 – Análisis por dimensión CIDAT**

Para cada una de las cinco dimensiones, se deberá analizar:

- ¿Qué impacto tendría la pérdida, degradación o fallo de dicha dimensión sobre la prestación del servicio o sobre la entidad?

- ¿Qué nivel de protección es necesario para mantener la operación segura y continua del dispositivo o sistema?

- **Paso 3 – Asignación de nivel por dimensión**

Cada dimensión deberá ser clasificada en una de las siguientes categorías:

- Bajo: Impacto reducido, sin afección significativa al servicio ni a la entidad.
- Medio: Impacto moderado, con afectación puntual o limitada en alcance.
- Alto: Impacto crítico o severo, con afección directa a la continuidad operativa, la seguridad de las personas, la integridad de los servicios o el cumplimiento normativo.

- **Paso 4 – Determinación del nivel global de criticidad**

El nivel de criticidad global corresponderá al más alto asignado en cualquiera de las dimensiones CIDAT, con el fin de garantizar que las medidas de protección se ajusten siempre al riesgo más crítico.

8.1.3. Ejemplos ilustrativos

A continuación, se incluyen dos ejemplos prácticos de aplicación del procedimiento:

- **Semáforo inteligente en una intersección vial**

La evaluación de las dimensiones de seguridad es la siguiente:

- Confidencialidad: Bajo (los datos no son sensibles).
- Integridad: Alto (si se manipula la programación, puede provocar accidentes viales).
- Disponibilidad: Alto (una caída del servicio impide la regulación del tráfico y puede generar incidentes graves).
- Autenticidad: Medio (es necesario asegurar que los comandos vengan de la autoridad competente).
- Trazabilidad: Medio (auditar cambios en la configuración es clave para investigar los incidentes).

Resultado: Criticidad Alta (al tener una dimensión valorada como alta).

- **Sensor de calidad del aire en un parque urbano**

La evaluación de las dimensiones de seguridad es la siguiente:

- Confidencialidad: Bajo (los datos son públicos).
- Integridad: Bajo (una alteración comprometería la calidad de la información publicada).
- Disponibilidad: Bajo (su ausencia afecta a la generación información en tiempo real, pero no se comprometen servicios esenciales).
- Autenticidad: Bajo (la procedencia de los datos es deseable, pero no crítica).
- Trazabilidad: Bajo (no es necesario auditar cada registro como si fuera evidencia crítica).

Resultado: Criticidad Baja (al ser todas las dimensiones valoradas como bajas).

8.2. Anexo II: Relación entre tipología de proveedores y clausulado

El presente anexo tiene por objeto proporcionar una herramienta práctica que permita seleccionar de forma clara y consistente las cláusulas de seguridad que deben incluirse en los pliegos de contratación, en función de la tipología del proveedor y del nivel de criticidad del dispositivo o sistema IoT evaluado.

Previamente, será necesario determinar la criticidad aplicable (baja, media o alta), conforme al procedimiento descrito en el “Anexo I. Guía para la clasificación de la criticidad de dispositivos y sistemas IoT “. Una vez establecida dicha criticidad, la tabla de este anexo permitirá identificar las cláusulas exigibles para cada caso, según las tipologías de proveedor definidas en el “Apartado 6. Tipologías de proveedores de tecnologías IoT en Smart Cities “.

La aplicabilidad se representa mediante un sistema de colores que refleja el nivel de criticidad del activo:

- **Verde:** Aplicable para criticidad alta, media y baja.
- **Naranja:** Aplicable para criticidad media y baja.
- **Rojo:** Aplicable para criticidad alta.

ID	Cláusulas	Suministradores de dispositivos IoT	Proveedores de servicios IoT	Proveedores mixtos
D_01	Gobernanza			
C_01_01	Asignación de Responsabilidades	●	●	●
C_01_02	Políticas y procedimientos	●	●	●
C_01_03	Gestión Documental	●	●	●
D_02	Cumplimiento normativo			
C_02_01	Normativa y conformidad	●	●	●

ID	Cláusulas	Suministradores de dispositivos IoT	Proveedores de servicios IoT	Proveedores mixtos
D_03	Gestión de usuarios y control de accesos			
C_03_01	Sistemas de Control de Acceso y Autenticación		●	●
C_03_02	Procedimientos de Autorización de Acceso		●	●
D_04	Gestión del acceso remoto para servicios de mantenimiento			
C_04_01	Autorización Previa para Herramientas de Acceso Remoto		●	●
C_04_02	Uso de Servicios VPN		●	●
C_04_03	Autenticación Multifactor		●	●
C_04_04	Autorización de Usuarios		●	●
C_04_05	Propuesta de Herramientas de Acceso Remoto para el Adjudicatario		●	●
C_04_06	Evaluación Excepcional de Herramientas de Acceso Remoto		●	●
D_05	Gestión de activos OT			
C_05_01	Clasificación de activos OT		●	●
C_05_02	Inventario de Activos	●	●	●

ID	Cláusulas	Suministradores de dispositivos IoT	Proveedores de servicios IoT	Proveedores mixtos
C_05_03	Control de Alta, Baja y Modificación de Activos		●	●
D_06	Configuración segura			
C_06_01	Configuración Inicial Segura		●	●
C_06_02	Deshabilitación de Servicios		●	●
D_07	Gestión de vulnerabilidades			
C_07_01	Proceso de Identificación y Gestión de Vulnerabilidades	●	●	●
C_07_02	Análisis Regular de Vulnerabilidades	●	●	●
C_07_03	Notificación y Plan de Corrección	●	●	●
C_07_04	Implantación Inicial Libre de Vulnerabilidades	●	●	●
D_08	Actualizaciones de software			
C_08_01	Políticas de Actualización	●	●	●
C_08_02	Actualizaciones Automáticas	●	●	●
C_08_03	Mecanismos Seguros de Actualización	●	●	●

ID	Cláusulas	Suministradores de dispositivos IoT	Proveedores de servicios IoT	Proveedores mixtos
C_08_04	Evaluación de Impacto y Pruebas	●	●	●
C_08_05	Documentación y Notificación	●	●	●
D_09	Desarrollo Seguro			
C_09_01	Seguridad desde el diseño	●	●	●
D_10	Mantenimiento físico de los dispositivos			
C_10_01	Coordinación con el equipo técnico y operativo		●	●
D_11	Acceso de emergencia autorizado al dispositivo			
C_11_01	Mecanismo de Acceso de Emergencia	●	●	●
D12	Seguridad contra el código dañino			
C_12_01	Uso de software antivirus y de Detección y Respuesta ante amenazas	●	●	●
D_13	Capacidad de bloqueo del dispositivo			
C_13_01	Niveles de Bloqueo Configurables	●		●
D_14	Gestión de eventos			

ID	Cláusulas	Suministradores de dispositivos IoT	Proveedores de servicios IoT	Proveedores mixtos
C_14_01	Registros de Seguridad y Configuración de Logs	●	●	●
C_14_02	Monitorización Continua y Revisión de Auditoría	●	●	●
D_15	Gestión de incidentes			
C_15_01	Proceso Integral de Gestión de Incidentes		●	●
C_15_02	Procedimientos de Contención y Recuperación		●	●
C_15_03	Notificación de Incidentes	●	●	●
C_15_04	Canales de Comunicación para Incidentes		●	●
D_16	Gestión segura de la cadena de suministro			
C_16_01	Evaluación de Terceros Proveedores relacionados con la adjudicación	●	●	●
C_16_02	Contratos y Acuerdos	●	●	●
D_17	Gestión de la obsolescencia			
C_17_01	Planificación de la Restitución y Transferencia Tecnológica		●	●
D_18	Protección de los servicios Cloud			

ID	Cláusulas	Suministradores de dispositivos IoT	Proveedores de servicios IoT	Proveedores mixtos
C_18_01	Localización y Ubicación Geográfica de los Datos Personales		●	●
C_19	Continuidad de negocio			
C_19_01	Política de Respaldo y Recuperación	●	●	●
C_19_02	Plan de Recuperación ante Contingencias	●	●	●
D_20	Auditorías técnicas y de cumplimiento			
C_20_01	Requisitos de Pruebas de Seguridad		●	●
C_20_02	Capacidad para Pruebas de Seguridad y Auditorías	●	●	●
C_20_03	Pruebas de Validación Post-Despliegue	●	●	●
D_21	Formación y concienciación en ciberseguridad			
C_21_01	Programas de Formación	●	●	●
C_21_02	Concienciación de Seguridad	●	●	●
D_22	Protección física de los dispositivos			
C_22_01	Protección Física de los Dispositivos	●	●	●

ID	Cláusulas	Suministradores de dispositivos IoT	Proveedores de servicios IoT	Proveedores mixtos
D_23	Comunicaciones seguras			
C_23_01	Configuración de Redes y Comunicaciones		●	●
D_24	Segmentación de la red urbana desplegada			
C_24_01	Segmentación por criticidad y función	●	●	●
C_24_02	Comunicaciones seguras y servicios expuestos	●	●	●
C_24_03	Protección de segmentos inalámbricos y redes municipales	●	●	●
D_25	Protección de la información			
C_25_01	Medidas de Seguridad para la Protección de Datos	●	●	●
D_26	Interoperabilidad segura con microservicios			
C_26_01	Configuración segura de APIs	●	●	●
D_27	Protección de los soportes de información			
C_27_01	Devolución y Destrucción de Datos		●	●
D_28	Integración segura con aplicaciones móviles			

ID	Cláusulas	Suministradores de dispositivos IoT	Proveedores de servicios IoT	Proveedores mixtos
C_28_01	Permisos y funcionalidades limitadas	●	●	●
C_28_02	Restricción de distribución de la aplicación en markets no autorizados	●	●	●
D_29	Integración con los Centro de Control Urbano o Plataforma Ciudad Inteligente			
C_29_01	Interfaces e interoperabilidad	●	●	●
C_29_02	Seguridad en la integración	●	●	●
C_29_03	Monitorización y gestión centralizada	●	●	●
D_30	Tratamiento de la información			
C_30_01	Transferencia de Conocimiento e Información al Finalizar el Contrato		●	●

TABLA 2: MAPEO DE TIPOLOGÍA DE PROVEEDORES CON LOS DOMINIOS/CLÁUSULAS.

9. Referencias y enlaces a información adicional

1. Boletín Oficial del Estado (BOE). (2018). *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*.
<https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673>
2. European Commission. (2025). *Procurement ecosystem factsheet (for medical devices)*.
<https://data.europa.eu/doi/10.2875/6879484>
3. European Commission. (2021). *Guidance on qualification and classification of software in Regulation (EU)*.
<https://ec.europa.eu/docsroom/documents/37581>
4. European Union. (2024). *Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements*.
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847>
5. International Organization for Standardization. (2022). *ISO/IEC 27400:2022: Cybersecurity — IoT security and privacy — Guidelines*.
<https://www.iso.org/standard/44373.html>
6. International Organization for Standardization. (2022). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.
<https://www.iso.org/standard/27001>
7. International Organization for Standardization. (2021). *ISO/SAE 21434:2021: Road vehicles — Cybersecurity engineering*.
<https://www.iso.org/standard/70918.html>
8. International Organization for Standardization. (2019). *ISO/IEC 27018:2019: Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*.
<https://www.iso.org/standard/76559.html>
9. International Organization for Standardization. (2019). *ISO 22301:2019: Security and resilience — Business continuity management systems — Requirements*.
<https://www.iso.org/standard/75106.html>

10. International Organization for Standardization. (2015). *ISO/IEC 27017:2015: Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*.
<https://www.iso.org/standard/43757.html>

10. Otras referencias de interés

El presente apartado recoge un resumen de los principales temas abordados en la guía, así como la relación de productos y servicios mencionados en ella. Su finalidad es ofrecer una visión global de los ámbitos tratados y facilitar la identificación de posibles referencias o elementos relevantes para futuras consultas o ampliaciones documentales.

10.1. Lista de materias tratadas en la guía

- Ciberseguridad aplicada a dispositivos conectados
- Internet de las Cosas (IoT) en Smart Cities
- Gestión de riesgos tecnológicos y regulatorios
- Cumplimiento normativo y marco regulatorio
- Gobernanza y gestión de la seguridad de la información
- Gestión de accesos, identidades y usuarios
- Protección de datos y privacidad
- Gestión de vulnerabilidades y actualizaciones de software
- Seguridad en la cadena de suministro y proveedores tecnológicos
- Configuración y mantenimiento seguro de dispositivos médicos
- Seguridad en redes, comunicaciones y servicios en la nube (Cloud)
- Gestión de incidentes y continuidad de negocio
- Formación, concienciación y cultura de ciberseguridad
- Interoperabilidad y seguridad en entornos digitales (APIs, apps, microservicios)
- Protección física de los dispositivos y de la información
- Auditorías, validación y mejora continua de la seguridad

10.2. Lista de productos mencionados en la guía

No se mencionan productos específicos en la guía.

10.3. Lista de servicios mencionados en la guía

No se mencionan servicios específicos en la guía.

Clausulado de seguridad para la contratación pública de tecnologías IoT en Smart Cities

Noviembre de 2025

Versión 1.0



Junta de Andalucía