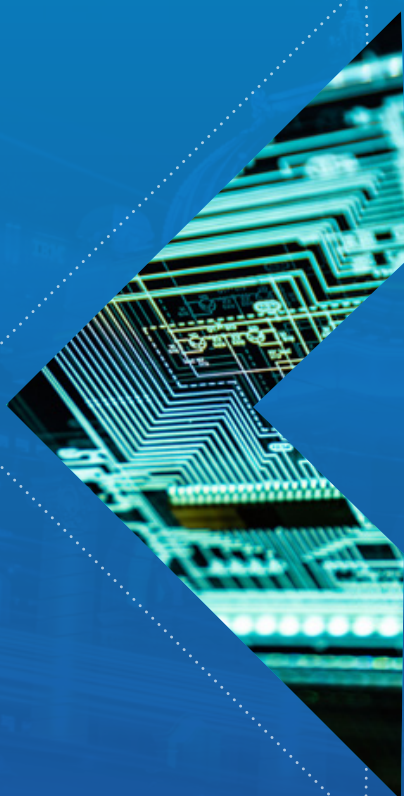


# Guía de *ciberseguridad*



para **ciudades inteligentes**



AUTORES: Lorenzo **Cotino**  
Marco **Sánchez**

EDITORES: Mauricio **Bouskela**  
Gilberto **Chona**  
Ariel **Nowersztern**  
Patricio **Zambrano-Barragán**  
Isabelle **Zapparoli**



# Guía de ciberseguridad para ciudades inteligentes

## **Autores:**

Lorenzo Cotino  
Marco Sánchez

## **Editores:**

Mauricio Bouskela  
Gilberto Chona  
Ariel Nowersztern  
Patricio Zambrano-Barragán  
Isabelle Zapparoli

Banco Interamericano de Desarrollo

**Catalogación en la fuente proporcionada por la  
Biblioteca Felipe Herrera del  
Banco Interamericano de Desarrollo**

Guía de ciberseguridad para ciudades inteligentes / Lorenzo Cotino, Marco Sánchez; editores, Maurício Bouskela, Gilberto Chona, Ariel Nowersztern, Patricio Zambrano-Barragán, Isabelle Zapparoli.

p. cm. — (Monografía del BID ; 963)

Incluye referencias bibliográficas.

1. Smart cities-Latin America. 2. City planning-Technological innovations-Latin America. 3. Computer security-Latin America. 4. Computer crimes-Latin America-Prevention. I. Cotino Hueso, Lorenzo. II. Sánchez, Marco. III. Bouskela, Maurício, editor. IV. Chona, Gilberto, editor. V. Nowersztern, Ariel, editor. VI. Zambrano-Barragán, Patricio, editor. VII. Zapparoli, Isabelle, editora. VIII. Banco Interamericano de Desarrollo. División de Vivienda y Desarrollo Urbano. IX. Banco Interamericano de Desarrollo. División de Innovación para Servir al Ciudadano. X. Serie.

IDB-MG-963

Códigos JEL: J18, K24, L86, L88, L90, L94, L95, L96, L98, M15, N96, O14, O18, O19, O31, O32, O38

Palabras clave: Ciberseguridad, ataques cibernéticos, ciberespacio, protección de datos, seguridad cibernética, gobernanza, protección de activos, ciudades, ciudades inteligentes, *smart city*, *smart cities*, sistemas de información, tecnologías de la información, Internet de las cosas, infraestructura urbana, servicios urbanos, América Latina y el Caribe, ALC, seguridad de la información, seguridad informática, transformación digital, CISO.

Esta guía de ciberseguridad para ciudades y gobiernos subnacionales proporciona conocimientos y recomendaciones para ayudar a las ciudades de América Latina y el Caribe (ALC) a protegerse en el ciberespacio. La guía está dirigida a los líderes de la ciudad, los gerentes y empleados municipales y el personal técnico en tecnologías de la información y la comunicación (TIC). Está dividida en cinco partes. Primero, aborda las generalidades de la ciberseguridad y los principales aspectos que la conforman, así como actores, riesgos e impactos. Segundo, incluye una hoja de ruta para comenzar a abordar la ciberseguridad a nivel local. Tercero, presenta una serie de recomendaciones dirigidas a las tres audiencias clave de la administración local. Cuarto, detalla información y referencias sobre modelos de gestión del riesgo, herramientas y otros instrumentos útiles para el personal técnico en TIC de un municipio. Por último, incluye el aporte del BID en la temática y presenta las conclusiones.

<https://www.iadb.org>

Copyright © 2021 Banco Interamericano de Desarrollo. Esta obra se encuentra sujeta a una licencia Creative Commons IGO 3.0 Reconocimiento-NoComercial-SinObrasDerivadas (CC-IGO 3.0 BY-NC-ND) (<https://creativecommons.org/licenses/by-nc-nd/3.0/igo/legalcode>) y puede ser reproducida para cualquier uso no-comercial otorgando el reconocimiento respectivo al BID. No se permiten obras derivadas.

Cualquier disputa relacionada con el uso de las obras del BID que no pueda resolverse amistosamente se someterá a arbitraje de conformidad con las reglas de la CNUDMI (UNCITRAL). El uso del nombre del BID para cualquier fin distinto al reconocimiento respectivo y el uso del logotipo del BID, no están autorizados por esta licencia CC-IGO y requieren de un acuerdo de licencia adicional.

Note que el enlace URL incluye términos y condiciones adicionales de esta licencia.

Las opiniones expresadas en esta publicación son de los autores y no necesariamente reflejan el punto de vista del Banco Interamericano de Desarrollo, de su Directorio Ejecutivo ni de los países que representa.



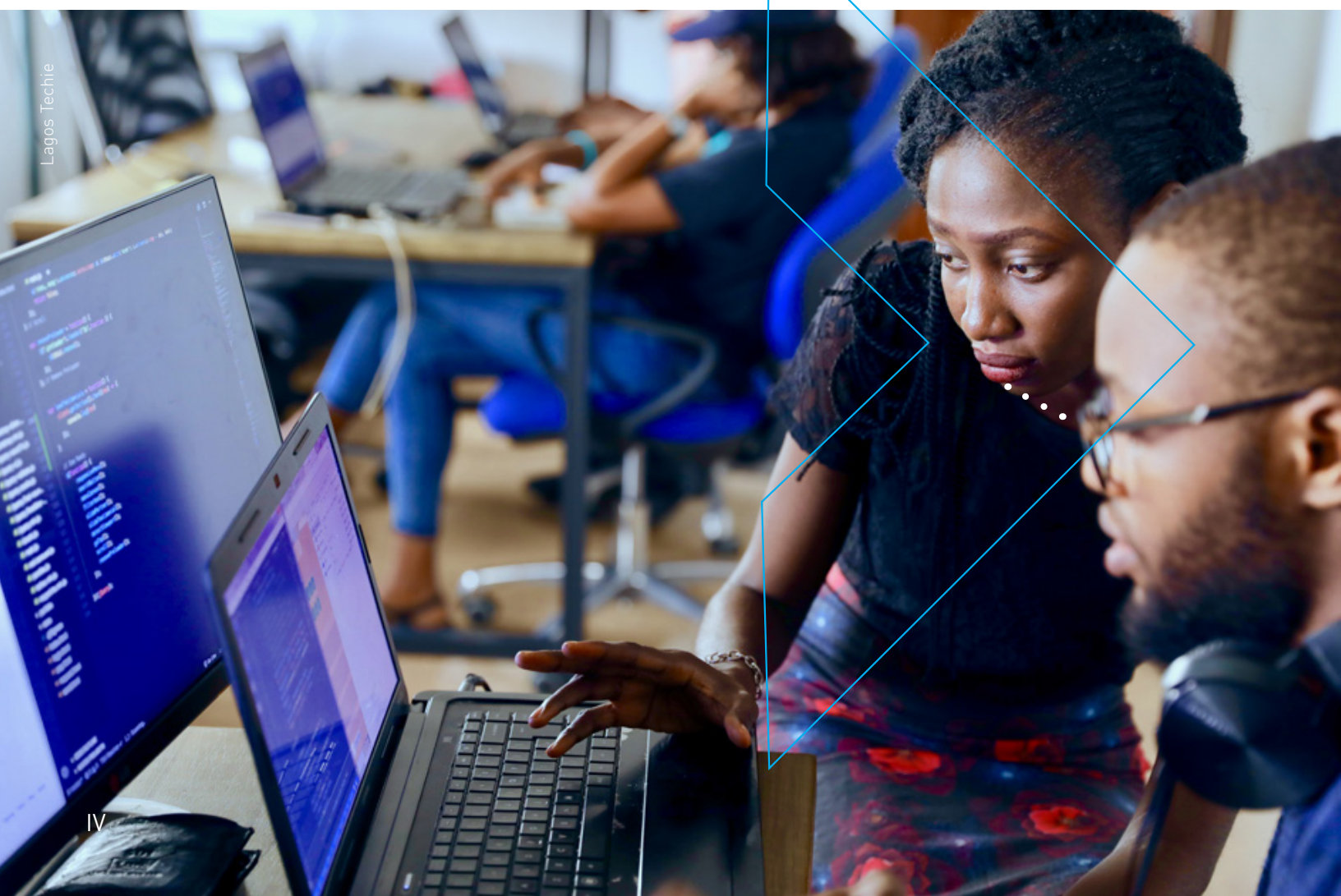
Revisión: Claudia M. Pasquetti y Sarah Schineller

Diseño: Ramón Zamora





**Esta guía de ciberseguridad para ciudades tiene por objetivo proporcionar conocimientos y valor agregado para comprender mejor la seguridad cibernética, los riesgos, los impactos potenciales y la urgencia de actuar de manera proactiva para proteger a las ciudades de América Latina y el Caribe.**







# Tabla de contenidos

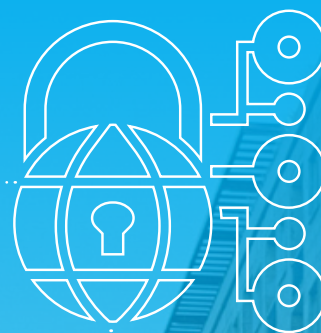
<b>Prefacio</b> .....	<b>VII</b>
<b>Prólogo y agradecimientos</b> .....	<b>XI</b>
<b>Introducción</b> .....	<b>1</b>
<b>Resumen ejecutivo</b> .....	<b>5</b>
<b>1. Ciberseguridad, ciberamenazas y su impacto en la ciudad</b> .....	<b>11</b>
<b>2. Recomendaciones y recursos para proteger las ciudades de los ciberataques</b> .....	<b>37</b>
<b>3. Decálogos para los niveles estratégico, táctico y operativo o técnico</b> .....	<b>67</b>
<b>4. Capacidades técnicas para brindar ciberseguridad a la ciudad</b> .....	<b>71</b>
<b>5. El BID y la ciberseguridad en las ciudades</b> .....	<b>83</b>
<b>Conclusiones</b> .....	<b>87</b>
<b>Referencias</b> .....	<b>89</b>







# Prefacio



Román López



**«Esta guía de ciberseguridad para ciudades es un aporte inicial a una discusión emergente que nos llevará a respuestas consistentes y contundentes ante el desafío que la ciberseguridad representa para el desarrollo resiliente, sostenible y equitativo de nuestras ciudades.»**





## Prefacio

La digitalización es una pieza central de la “Visión 2025:<sup>1</sup> Reinvertir en las Américas” del Banco Interamericano de Desarrollo (BID) y se basa en la idea de que aprovechar al máximo el inmenso potencial de la transformación digital requiere pensamiento estratégico de largo plazo, una mejor conectividad, fortalecimiento de la gobernanza digital, fomento de la innovación, más capital humano, una infraestructura digital más sólida y la actualización de regulaciones obsoletas que rigen las tecnologías de la información y la comunicación (TIC).

**Con el advenimiento de la pandemia de COVID-19, el proceso de digitalización a nivel global se aceleró marcadamente, y trajo aparejados cambios importantes en la forma de vivir, de trabajar y de comunicarse. De este modo, aumentó el grado de digitalización en las empresas, los hogares y los servicios públicos.**

Esto ha introducido nuevas formas de acceso a la información y a los servicios, ha abierto nuevos canales de comunicación entre gobierno y ciudadanos; y brinda oportunidades para mejorar la gobernanza en general.

Las áreas metropolitanas y los municipios no son ajenos a este cambio en el paradigma digital. De hecho, las ciudades son un agente cada vez más importante del proceso de digitalización mundial. La adopción de las nuevas tecnologías digitales es una característica esencial para el desarrollo de las ciudades y un motor de innovación, mayor comunicación, colaboración, equidad y eficiencia.

Sin embargo, a medida que crece la digitalización de la gestión gubernamental local, de infraestructura y de servicios urbanos, crece también la exposición al riesgo y la vulnerabilidad ante ciberataques. Es decir, la dependencia de las TIC para gestionar y monitorear sistemas esenciales que sustentan áreas clave como seguridad, agua, energía, movilidad y atención a los eventos catastróficos relacionados con el cambio climático incrementa los niveles de riesgo de ciberataques.

.....

1. Véase el enlace <https://www.iadb.org/es/acerca-del-bid/perspectiva-general>.



Rápidamente, la ciberseguridad en las ciudades se ha convertido en un elemento clave de su buena gobernanza. Los ciberataques tienen un alto potencial de interrumpir las operaciones de las ciudades, afectar sus finanzas y la reputación de la administración, y provocar un daño significativo a los sistemas de información por tiempo indefinido. Estos ataques cibernéticos amenazan la continuidad de los servicios, el acceso expedito a la información, la privacidad de los datos personales y los medios de pago digitales que utilizan los municipios y los ciudadanos, entre otras áreas críticas.

Inevitablemente, las ciudades siguen expuestas a brechas de ciberseguridad. Aunque muchas ciudades han sido objeto de ciberataques, todavía existen retos y desafíos en la gobernanza y gestión del riesgo para abordar la ciberseguridad de forma proactiva, especialmente a nivel municipal.

Los datos disponibles indican claramente que los ciberataques y los incidentes, en particular aquellos perpetrados con intención delictiva, están aumentando en frecuencia y sofisticación, y pueden tener costos muy elevados. Además, el ciberdelito no reconoce las fronteras nacionales y es un problema que concierne a todas las organizaciones del sector público (nacional o subnacional) y del sector privado.

Recientemente, el BID ha realizado importantes esfuerzos para abordar las brechas de conocimiento en ciberseguridad y ayudar a los organismos públicos nacionales y las empresas privadas a mejorar sus marcos, medidas y capacidades para reforzar la ciberseguridad, a la par de la necesidad de profundizar la cooperación y el intercambio de información.

Los principales desafíos para abordar la vulnerabilidad de las ciudades a los delitos cibernéticos están relacionados con una débil gobernanza, y una falta de sensibilización sobre la gravedad de los riesgos y potenciales daños de un posible ataque cibernético. Además, la limitada asignación de recursos en un contexto de presupuestos restringidos frente a múltiples prioridades, así como la carencia de recursos humanos calificados, añade gravedad al problema.

Para las ciudades de la región, la cuestión no es “si” va a ocurrir un ciberataque: la cuestión es “cuándo” va a ocurrir. Las ciudades pueden planificar de forma proactiva para que los ciberataques no generen interrupciones en su gobernanza y su gestión administrativa.



Goh Rhy Yan

**La exploración de la ciberseguridad en las ciudades que se presenta en esta publicación busca promover el conocimiento y las acciones de protección cibernética para las urbes de América Latina y el Caribe (ALC), a través de un tratamiento franco y abierto del tema, de modo que sirva a los encargados de la toma de decisiones de las ciudades como una guía inicial para fortalecer su proceso de digitalización, y al mismo tiempo reducir la vulnerabilidad a los ciberataques.**

Específicamente, esta guía ayudará a aumentar la conciencia sobre la importancia de consolidar los marcos y procesos de ciberseguridad de las ciudades; entre otras herramientas, concretamente, propone una hoja de ruta y un plan de acción necesarios para las ciudades de ALC.

Esta guía de ciberseguridad para ciudades es un aporte inicial a una discusión emergente que nos llevará a respuestas consistentes y contundentes ante el desafío que la ciberseguridad representa para el desarrollo resiliente, sostenible y equitativo de nuestras ciudades. Buscamos mejorar vidas en ciudades cada vez más digitalizadas y queremos hacerlo de forma segura.



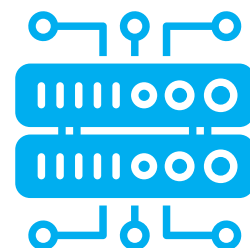
**Tatiana Gallego Lizón**

Jefa de la División de Vivienda y Desarrollo Urbano  
Sector de Cambio Climático y Desarrollo Sostenible  
Banco Interamericano de Desarrollo



**Edgardo Mosqueira Medina**

Jefe de la División de Innovación para Servir al Ciudadano (a.i.)  
Sector de Instituciones para el Desarrollo  
Banco Interamericano de Desarrollo





# *Prólogo y agradecimientos*



Jurriaan

*«Los gobiernos municipales aprovechan cada vez más la tecnología digital, Internet y la tecnología móvil para planificar, conectar y gestionar la infraestructura y los servicios urbanos, y así mejorar la calidad de vida de sus habitantes.»*



# Prólogo y agradecimientos

**Esta guía surgió de la reflexión del BID sobre cómo apoyar a las ciudades de la región para que puedan protegerse en el ciberespacio mientras transforman su modelo de gestión tradicional para convertirlo en un modelo inteligente.**

Los gobiernos municipales aprovechan cada vez más la tecnología digital, Internet y la tecnología móvil para planificar, conectar y gestionar la infraestructura y los servicios urbanos, y así mejorar la calidad de vida de sus habitantes. Con la pandemia, se agilizó la digitalización de las ciudades. Ciudades más conectadas es a la vez sinónimo de ciudades más expuestas. El riesgo de ser objetivo de ciberataques es cada vez mayor. El costo económico de paralizar el funcionamiento de la ciudad es muy alto, y pone en riesgo no solo la infraestructura y los servicios urbanos sino también la seguridad de los ciudadanos.

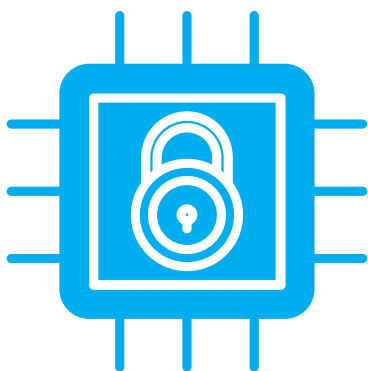
La preparación de esta guía fue un esfuerzo conjunto de los departamentos de Cambio Climático y Desarrollo Sostenible (CSD), Instituciones para el Desarrollo (IFD) y Conocimiento, Innovación y Comunicación (KIC), liderados por Juan Pablo Bonilla, Moisés Schwartz y Federico Basaños, respectivamente. La supervisión técnica provino de la División de Vivienda y Desarrollo Urbano (CDS/ HUD) y de la División de Innovación para Servir al Ciudadano (IFD/ ICS), bajo la égida de Tatiana Gallego Lizón y de Edgardo Mosqueira Medina (a.i.), respectivamente. La coordinación estuvo a cargo de Mauricio Bouskela, Gilberto Chona y Ariel Nowersztern, con el apoyo de Isabelle Zapparoli, quienes realizaron la edición del texto, con las contribuciones de Patricio Zambrano-Barragán y Miguel Ángel Porrúa como revisores de contenido y enfoque.

Los autores, Lorenzo Cotino Hueso (España) y Marco E. Sánchez Acevedo (España-Colombia), son profesores universitarios y expertos legales en ciberseguridad y uso de TIC por parte de las administraciones públicas; con ellos, el equipo coordinador seleccionó los temas críticos de la ciberseguridad, las características y las recomendaciones, todo ello orientado a tres audiencias de las administraciones locales: los líderes de la ciudad, los gerentes y empleados municipales y el personal técnico en TIC.





**El tema de la ciberseguridad tiene muchas aristas; existen estudios de casos, modelos y ámbitos de acción. Sin embargo, en esta primera edición, la guía sintetiza los temas críticos de la ciberseguridad en los cuales deben enfocarse las tres audiencias urbanas ya mencionadas.**



Esta guía sobre ciberseguridad para ciudades inteligentes fue financiada con fondos del programa Cutting-Edge del Departamento KIC (VPS/KIC). Agradecemos el apoyo de Pablo Alzuri, Allen Blackman, Andrés Blanco, Janaina Borges, Hallel Elnir, Luis Manuel Espinoza, Andrea Florimon, Kenneth Foley, Jessica Guzmán Osorio, Cristina Hinojosa Lecaros, Philip Keefer, Kidae Kim, Pablo Libedinsky, Nora Libertun, Ángel Macuare Herrera, Marcelo Madeira da Silva, Fernando Melean, Santiago Paz, Daniel Peciña López, Lorena Rodríguez Bu y Sarah Schineller por su asesoramiento y apoyo durante el desarrollo de la propuesta, el financiamiento, los procesos internos, y la comunicación estratégica relacionada con la publicación.

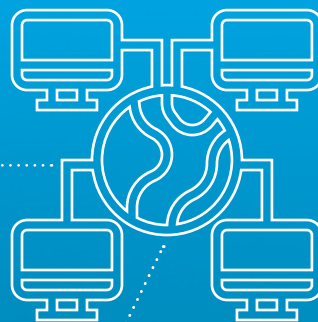
El equipo agradece a los gestores y equipos técnicos de las ciudades de ALC, quienes, a lo largo de los años, a través del diálogo, la implementación de proyectos y la participación en estudios nos han compartido su preocupación por mejorar los servicios en las ciudades y nos han ayudado a generar contenidos de la agenda de política urbana de la región.







# Introducción



Marck Maciel

**«Las ciudades utilizan cada vez más el ciberespacio, una compleja infraestructura de redes de conectividad e interfaces de comunicación, de sensores y dispositivos conectados, así como también de centros de operación y control.»**



# Introducción

Con el objetivo de aumentar la conciencia y la comprensión acerca de la seguridad cibernética o ciberseguridad, así como de los riesgos potenciales y los resultados de los ataques cibernéticos en las operaciones de las ciudades, el BID presenta esta guía, que permite visualizar los riesgos, los impactos potenciales y la urgencia de administrar las ciudades de la región para protegerse de esos ataques.

**La ciberseguridad debe ocupar un lugar prioritario en la agenda de los líderes de las ciudades y los gobiernos nacionales, regionales y locales.**

## ¿Qué es la guía de ciberseguridad para ciudades inteligentes?

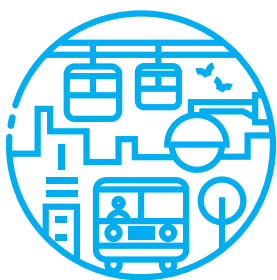


Esta guía de ciberseguridad para ciudades y gobiernos subnacionales (en adelante, gobiernos) proporciona conocimiento para las ciudades de ALC sobre la ciberseguridad, los riesgos digitales, los impactos potenciales y la urgencia de actuar de manera proactiva.

Esta guía forma parte del apoyo que el BID proporciona a las ciudades de ALC en su transformación digital, y constituye un complemento de otras publicaciones, entre las que cabe citar: [La ruta hacia las Smart Cities: migrando de una gestión tradicional a la ciudad inteligente \(2016\)](#); [Big Urban Data: A Strategic Guide for Cities \(2019\)](#); [Políticas públicas orientadas por datos: los caminos posibles para gobiernos locales \(2020\)](#) y [Big Data para el Desarrollo Urbano Sostenible \(2021\)](#).

A la vez, la guía también forma parte del corpus de conocimiento especializado extendido por el BID en el tema emergente de la ciberseguridad en distintos sectores, entre ellos, energía, salud, agua y cumplimiento de la ley, con lo cual se procura colaborar a fin de cerrar la brecha de conocimiento que impide su desarrollo digital. En la publicación [Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe](#), el BID y la Organización de Estados Americanos (OEA) describen detalladamente la madurez de los países de ALC en ciberseguridad, así como las oportunidades de mejora.





## ¿Para quién es esta guía?

La **Guía de ciberseguridad para ciudades inteligentes** está dirigida a tres tipos de usuarios dentro de las ciudades (véase el gráfico 1).

Gráfico 1.

# Usuarios de la guía de ciberseguridad para ciudades



Fuente: Elaboración propia (2021).

## ¿Qué objetivos persigue esta guía?

Los objetivos de la guía son los siguientes:



1. **Ayudar a las ciudades** y administraciones locales de la región de ALC a protegerse en el ciberespacio.
2. **Aumentar la conciencia** y la comprensión de la seguridad cibernética, a fin de resguardar la protección de la información de cada ciudad y la continuidad de los servicios y de la infraestructura.
3. **Proporcionar conocimientos** sobre los riesgos potenciales y la adopción de medidas de seguridad para reducir la probabilidad de ataques cibernéticos, así como minimizar el impacto en caso de incidentes.

## ¿Cómo se encuentra estructurada esta guía?

La guía de ciberseguridad para ciudades está organizada en **cinco capítulos**, que ofrecen un camino para que los líderes gubernamentales, los gerentes municipales y el personal técnico encargado de la ciberseguridad y las TIC, así como también terceras partes, puedan transformar positivamente sus ciudades en ciudades seguras e inteligentes.

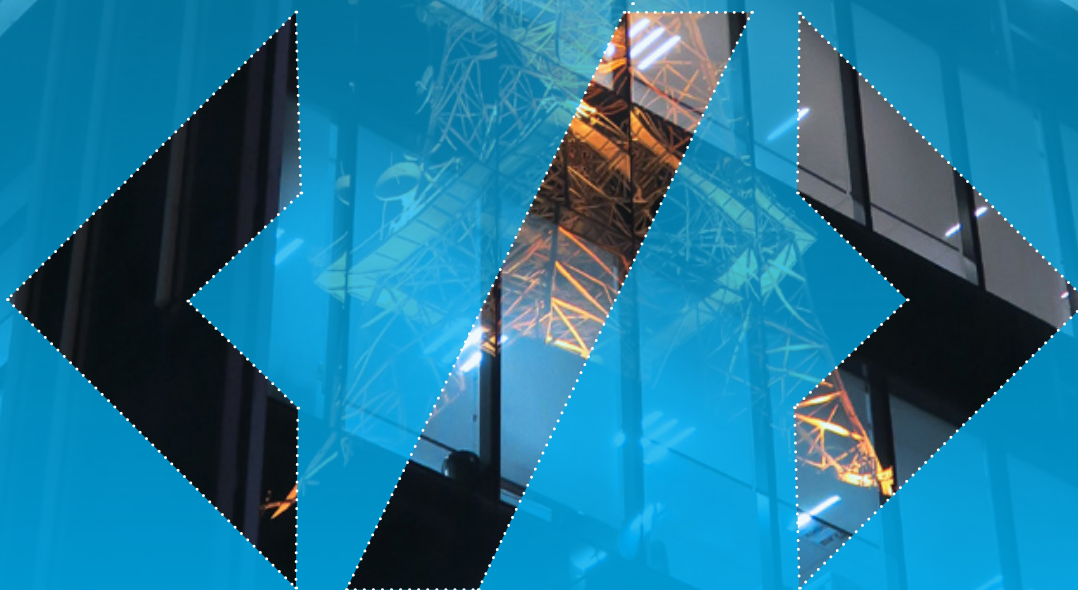
A continuación, se presenta un resumen ejecutivo, que contiene la estructura esencial de los elementos abordados a lo largo del documento. Luego, en el [capítulo 1](#), se define qué es la ciberseguridad, se proporciona un contexto, y se describen el ecosistema, las motivaciones, los actores, las amenazas, las vulnerabilidades, y el impacto que un ataque puede generar a nivel municipal. En el [capítulo 2](#), se abordan las mejores prácticas, la hoja de ruta, la gobernanza, la institucionalización de la ciberseguridad, la relación con la cadena de proveedores, así como la formación, la cultura y el financiamiento de proyectos de ciberseguridad. En el [capítulo 3](#), se presenta un conjunto de recomendaciones dirigidas al personal estratégico, táctico y operativo, técnico y conformado por terceros de apoyo, para hacer frente a las amenazas que genera el actuar por medio de las TIC. En el [capítulo 4](#), se desarrollan las capacidades técnicas necesarias para dar ciberseguridad a la ciudad. En el [capítulo 5](#), se presenta el ámbito de acción del BID en materia de ciberseguridad dentro del contexto de promoción de la digitalización de la región y las ciudades inteligentes.

# *Resumen ejecutivo*

---



Fabio Hanashiro



*«La ciberseguridad óptima es invisible,  
porque anticipa y elimina problemas.»*

# Resumen ejecutivo

**Los alcaldes y sus concejos municipales están liderando la transformación digital de la ciudad para prestar mejores servicios y gestionar la infraestructura urbana, así como mejorar la autonomía financiera, la sostenibilidad y la gobernabilidad.**



**Las ciudades utilizan cada vez el ciberespacio**, una compleja infraestructura de redes de conectividad e interfaces de comunicación, de sensores y dispositivos conectados, de centros de operación y control. Esta digitalización va acompañada de proyectos de ciudades inteligentes o conectadas. Incluso se utiliza inteligencia artificial y tecnologías emergentes para captar y explotar datos para monitorear, proponer o adoptar decisiones para las urbes y sobre la ciudadanía.

**Pero esta transformación digital atrae cada vez más a los ciberatacantes a las ciudades**, también en ALC. Sin embargo, la gran mayoría de los alcaldes, altos directivos, integrantes del personal y la ciudadanía misma no son conscientes de las vulnerabilidades en materia de ciberseguridad que tienen las ciudades. Cada día, se producen cientos de miles de ciberataques. Afortunadamente, la mayor parte es repelida gracias a acciones de ciberseguridad. En algunas ocasiones el público se ve impactado por noticias de robos de datos de la ciudad, ataques a sus sistemas de transporte, de emergencia o policía, así como a sus hospitales. Ha habido ciudades completas sometidas al chantaje e inoperativas durante semanas (Baltimore) o dimisiones de altos responsables municipales por no invertir a tiempo (Atlanta). Incluso se han producido episodios de violencia urbana como consecuencia de ataques de desinformación.

**La ciberseguridad óptima es invisible, porque anticipa y elimina problemas.** No hay que esperar a que sucedan los desastres para protegerse. Hay que prevenirlos y saber cómo actuar si se producen. Interrumpir los servicios públicos y la infraestructura crítica de la ciudad tiene un costo social, económico, político y reputacional muy alto para cualquier urbe.

**Con esta guía se apunta a sensibilizar y comprender las ciberamenazas para poder pasar a la acción.** Así, se ofrecen los que se consideran como algunos de los mejores instrumentos y recomendaciones, una hoja de ruta para seguir y elementos básicos para actuar de modo proactivo frente a las ciberamenazas. Se establece el camino para que líderes, alcaldes y altos directivos, así como empleados, técnicos y terceras partes puedan transformar sus ciudades en lugares más ciberseguros.



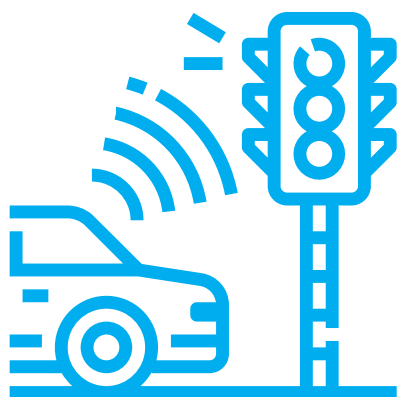




Chuttersnap

En el **primer capítulo**, se explica qué es la ciberseguridad, qué son las ciberamenazas y cuál es el impacto de los ciberataques a ciudades. La ciberseguridad supone proteger datos, información, *hardware*, *software*, servicios, recursos humanos, instalaciones e infraestructura crítica. En ella están implicados todos los actores de una ciudad inteligente, por lo que su finalidad es reducir los riesgos o amenazas cibernéticos ante los que están expuestos autoridades, ciudadanos y empresas cuando realizan sus actividades o cumplen sus funciones en el ciberespacio.

No es nada fácil saber por qué los cibercriminales, ciberespías, ciberterroristas, ciberactivistas o quiénes quiera que sean realizan sus ataques (a instituciones, gobiernos, entes privados, empresas, países), ni cuáles son sus motivaciones (políticas, delictivas, económicas o empresariales, o meramente personales). Somos vulnerables por fallas del *software*, de infraestructura muchas veces obsoleta, porque no sabemos o no entendemos nuestras vulnerabilidades, no comprendemos el ecosistema tecnológico de la ciudad. No es fácil gobernar y orquestar a los numerosos actores participantes, ni saber y compartir la información de seguridad y de los incidentes o fallas cuando acontecen. Los atacantes aprovechan en sus víctimas la falta de estrategias, de planes de gestión de riesgos y de gestión de incidentes. Y las vulnerabilidades humanas son, por lo general, más importantes que las tecnológicas. No se conocen ni se contratan recursos humanos con los nuevos perfiles profesionales que se requieren; los ataques se producen especialmente porque no se crea conciencia, no se sensibiliza ni se brinda capacitación ni formación a los directivos, al personal de las dependencias públicas ni a la ciudadanía misma.



En este capítulo se exponen algunos ataques informáticos, ocurridos en el mundo y también en ALC, que han paralizado ciudades y generado altos costos, e incluso han llevado a la dimisión de sus gobernantes. Estos casos deben crear conciencia acerca de la trascendencia de la ciberseguridad en las ciudades y pueden servir para que los responsables estratégicos, tácticos y tecnológicos u operativos queden más convencidos de la necesidad de pasar a la acción. La COVID-19 ha intensificado los ciberataques. Las vulnerabilidades se han incrementado, debido al teletrabajo sin suficientes medidas de protección y a nuevas formas de ingeniería social surgidas a partir de inquietudes y necesidades generadas por la enfermedad, o se ha atacado o chantajeado a centros y sistemas de salud, entre otras modalidades ofensivas.

El **segundo capítulo** brinda algunas recomendaciones y describe buenas prácticas que conforman una posible hoja de ruta que cualquier ciudad puede seguir para lograr la mejor ciberseguridad posible. Asimismo, se delinean los perfiles de los responsables de

implementar estas acciones. Todo parte de identificar los activos y los actores; debido a la complejidad de la ciudad que se deba proteger y a los numerosos sujetos que intervienen, se necesita una gobernanza de la ciberseguridad, que esté integrada en la gobernanza de la ciudad inteligente y en la más amplia gobernanza del dato.

La seguridad digital de la ciudad ha de estar conectada, apoyada y articulada por las políticas y estrategias nacionales de ciberseguridad; se la debe institucionalizar. Ello no es lo habitual. Ahora bien, una ciudad puede ser pionera si proactivamente coopera en materia de conocimiento e incorpora las mejores prácticas de los niveles internacionales, nacionales, regionales y también locales. Si lo hace, podrá además acceder a los mejores recursos y fuentes de financiamiento. La gobernanza de la ciberseguridad parte de la legislación que se debe cumplir. En la guía se mencionan algunas leyes específicas; de igual modo, hay que conocer los estándares de ciberseguridad de referencia y optar por el más adecuado y posible para la ciudad. A partir de estas bases, el nivel estratégico ha de desarrollar políticas y normas de seguridad para todos los actores, y establecer competencias claras. Por supuesto, todas las partes deben involucrarse para hacer propias estas políticas y normas. Se recomienda centralizar la responsabilidad de la ciberseguridad en una persona u oficina.

**La hoja de ruta por seguir también implica que hay que dotar de seguridad a los datos y a la información según su nivel de riesgo, lo cual es especialmente válido para los datos confidenciales o personales.**

Una de las mayores barreras para la ciberseguridad es la falta de confianza o de instrumentos y plataformas que permitan compartir la información de seguridad y de incidentes entre las partes. Frente a ello, aquí se exponen algunos modelos y buenas prácticas por seguir para organizar e intercambiar información.

La colaboración público-privada es esencial para la transformación digital de las ciudades y también para su ciberseguridad. Por ello, esta guía contiene recomendaciones concretas para integrar la ciberseguridad en la contratación de prestadores y en el suministro de productos y servicios tecnológicos para la ciudad, con una descripción concreta de los servicios que han de incluirse, la atención, la información que ha de compartirse, la obligación de que los productos y servicios sean seguros en cuanto al diseño, y cumplan la normativa y los estándares. Asimismo, se presenta una serie de recomendaciones útiles para elegir la empresa o el prestador de servicios de la ciudad inteligente.



Como se ha adelantado, el factor humano es incluso más importante que las medidas técnicas de ciberseguridad. Por lo tanto, resulta imprescindible una cultura de seguridad, concienciación y formación, todo lo cual empieza por el alcalde y su concejo, pasa por los altos directivos y los responsables de la ciudad inteligente, más todos los empleados y técnicos en tecnología, y concluye con toda la ciudadanía. Se recomienda poner especial énfasis en una buena comunicación de todas las acciones que se emprendan entre todos los sujetos involucrados. Finalmente, no cabe duda de que la ciberseguridad necesita un financiamiento planificado, financiamiento que inevitablemente habrá de aumentar, si no se destinan recursos a tiempo. También se señala la posibilidad de contratar seguros para la ciberseguridad urbana.

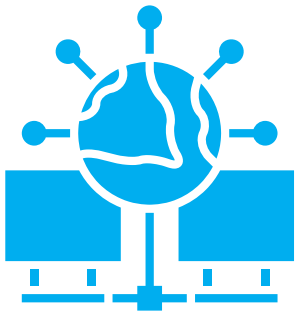


En el **tercer capítulo**, se proponen tres decálogos para lograr la ciberseguridad para los tres perfiles inicialmente mencionados.

En primer lugar, se presentan recomendaciones a **nivel estratégico** (alcaldes y altos directivos) desde una visión urbana y a mediano y largo plazo; se enfatiza la necesidad de poner el tema en la agenda de políticas para poder asignar recursos sin esperar a sufrir un ataque; reforzar las acciones con normas, competencias claras y la institucionalización de liderazgos y órganos que tengan recursos adecuados. Se debe estimular que las medidas preventivas se lleven a la práctica y no se queden en los “cajones”. El liderazgo debe ejercerse también sobre el sector privado que presta servicios y suministros a la ciudad. Hay que vigilar la renovación de equipos obsoletos, los cuales deben ser reemplazados por equipos nuevos que sean ciberseguros. La privacidad y la ciberseguridad se han de integrar en las evaluaciones de la ciudad inteligente, y habrá que adoptar estrategias y asociarse con redes de ciberseguridad nacionales e incluso internacionales.

También se presenta un decálogo para el **nivel táctico** (secretarios municipales y empleados). En este caso, se requiere un buen conocimiento de los sistemas e infraestructuras que hay que proteger y de las amenazas principales que pueden sufrir. Para ello, resulta de especial utilidad llevar a cabo una autoevaluación que permita determinar las capacidades faltantes. Asimismo, los secretarios municipales deben conocer las acciones concretas, las estrategias, las normas, las políticas y los procedimientos de ciberseguridad que tiene la ciudad; también deben tener claras sus responsabilidades al respecto, y comunicar las responsabilidades que atañen a los órganos y al personal de la ciudad. De igual modo, se ha de velar porque las medidas previstas se pongan a prueba. Los secretarios deben tener la formación adecuada, y contar con financiamiento y recursos humanos estructurados, planificados





y suficientes. En cuanto a los proveedores y prestadores privados, hay que concretar obligaciones y al mismo tiempo crear un clima de confianza que permita compartir información crítica de ciberseguridad.

Para el **nivel operativo** (personal con responsabilidades o labores vinculadas a la tecnología, personal con capacidades tecnológicas y terceros de apoyo) también hay un decálogo. Este incluye determinar la información y los activos que se deben proteger, y participar activamente en la evaluación, gestión y planificación de la ciberseguridad como un proceso continuo. La labor técnica tiene especial protagonismo para que haya sistemas de identificación, autenticación fuerte de dos factores (control y acceso), y mecanismos de detección de anomalías y vigilancia para dar respuesta a incidentes. También se debe vigilar que los bienes y servicios incluyan la seguridad y privacidad que corresponda en el diseño y por defecto. De igual modo, es importante estar al día en los métodos y herramientas de los atacantes, así como contar con sistemas automatizados para detectar y dar respuesta a las amenazas. Asimismo, hay que velar porque el *hardware* y el *software* estén actualizados, e integrar las acciones de privacidad y protección de datos con las de ciberseguridad.

El **cuarto capítulo** contiene un apartado especialmente dirigido a los responsables y expertos tecnológicos. Así, se agrupan los aspectos técnicos de la ciberseguridad con una descripción del ciclo y pasos por seguir (gestión, identificación, protección, detección, respuesta, recuperación y autoevaluación). Se exponen, para un público de perfil tecnológico, los elementos técnicos de la planificación basada en capacidades, así como la hoja de ruta y los principales modelos de madurez de capacidades y las funciones de ciberseguridad, equipos y tecnología para gestionar cotidianamente la ciberseguridad en una ciudad. Por último, se detallan las responsabilidades que deben atribuirse a este grupo de alto nivel encargado de la ciberseguridad.

Finalmente, el **quinto capítulo** ilustra cómo el BID articula la ciberseguridad con su visión y ámbito de acción, sobre la base de la promoción de las ciudades inteligentes al servicio de los ciudadanos. Seguidamente, se resumen ciertas conclusiones generales. Así, se remarca la esencia de la ciberseguridad: el conocimiento y la comprensión del entorno, la planificación, la proactividad en materia de prevención y la constante vigilancia, la colaboración y cooperación, el entrenamiento y la capacitación permanentes. Solo bajo estos principios se podrán aprovechar las ventajas de las tecnologías disruptivas para tener ciudades más sostenibles, inclusivas, productivas y mejorar las vidas de los ciudadanos.

# 1

## ***Ciberseguridad, ciberamenazas y su impacto en la ciudad***



NASA



***«La ciberseguridad supone proteger datos,  
información, hardware, software, servicios,  
recursos humanos, instalaciones  
e infraestructura crítica.»***



# 1

## Ciberseguridad, ciberamenazas y su impacto en la ciudad

A partir del siglo XXI, el uso de TIC se ha convertido en un elemento central de las ciudades, de los Estados y del ejercicio de los derechos ciudadanos. Cada urbe ha iniciado su camino de transformación digital hacia lo que se ha denominado ciudad inteligente o *smart city*. Según Bouskela et al. (2016), una ciudad inteligente es aquella que coloca a las personas en el centro del desarrollo, incorpora TIC en la gestión urbana y utiliza estos elementos como herramientas para estimular la formación de un gobierno eficiente que incluya procesos de planificación colaborativa y participación ciudadana. Al promover un desarrollo integrado y sostenible, las *smart cities* se tornan más innovadoras, competitivas, atractivas y resilientes, lo cual contribuye a mejorar las vidas de sus habitantes.

**La ciudad que hay que proteger cuenta con ciertos elementos fundamentales: un ecosistema urbano inmerso en una región; un conjunto que abarca infraestructura, sistemas, plataformas y redes; una ciudadanía que interactúa, ejerce sus derechos y busca la satisfacción de sus necesidades. (Enerlis et al., 2012)**

Estas ciudades tienen un nuevo entorno, el ciberespacio, es decir: “un entorno complejo que consta de interacciones entre personas, *software* y servicios de Internet por medio de dispositivos tecnológicos y redes conectados a ella, y que no existe en forma física” (ISO, 2012).

# El ciberespacio como entorno complejo

Jezael Melgoza

Ciberespacio

Centro de operación y control

Software

Sensores y dispositivos

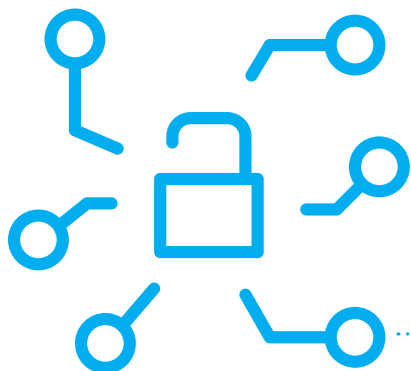
Conectividad e interfaces

Personas

Fuente: Elaboración propia (2021).

Anna Dziubinska





## 1.1

# ¿Qué es la ciberseguridad?

La ciberseguridad enfrenta los riesgos asociados a la prestación de servicios en el ciberespacio. La Unión Internacional de Comunicaciones (UIT, 2018: Cláusula 3.2.5) propone la siguiente definición de ciberseguridad:

*«El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno».*

*«Los activos de la organización y de los usuarios son los dispositivos informáticos conectados, el personal, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno».*

*«La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno».*



Arlington Research

El término “ciberseguridad” abarca todas las dimensiones de la seguridad digital (OCDE, 2015): **1) la tecnología**, cuando se centra en el funcionamiento del entorno digital (a menudo llamado “seguridad de la información”, “seguridad informática” o “seguridad de la red” por los expertos); **2) la aplicación de la ley o aspectos legales** (por ejemplo, ciberdelito); **3) la seguridad nacional, la estabilidad internacional**, incluidos aspectos como el papel de las TIC respecto de la inteligencia, la prevención de conflictos, la guerra, la ciberdefensa, etc., y **4) la dimensión económica y social**, que abarca la creación de riqueza, la innovación, el crecimiento, la competitividad y el empleo en todos los sectores económicos, las libertades individuales, la salud, la educación, la cultura, la participación democrática, la ciencia, el ocio y otras dimensiones del bienestar en que el entorno digital impulsa el progreso.

La ciberseguridad en una ciudad inteligente es **la capacidad de las autoridades, los ciudadanos y las empresas para reducir los riesgos o amenazas cibernéticas ante los que están expuestos cuando realizan sus actividades o cumplen sus funciones en el ciberespacio.**



La ciberseguridad busca la protección de los activos digitales del ecosistema urbano y, para conseguir esta finalidad, se deben identificar los siguientes elementos:

- 1 ① **La gobernanza**, políticas y lineamientos.
- 2 ② **Los actores** y usuarios.
- 3 ③ **El entorno**.
- 4 ④ **La colaboración** y articulación con el entorno.
- 5 ⑤ **Las herramientas** y los instrumentos tecnológicos utilizados y que dan soporte a la prestación de los servicios.
- 6 ⑥ **Las metodologías** aplicadas y buenas prácticas para la gestión del riesgo y el manejo de incidentes.
- 7 ⑦ **La formación** y la capacitación permanentes.

Se pueden distinguir dos tipos de activos relacionados con la seguridad de la información (ISO, 2018): los **activos principales** (procesos y actividades de negocios e información) y los **activos de apoyo** (de los que dependen los activos primarios) de todo tipo: *hardware*, *software*, red, personal, sitios (portales web o infraestructura física), estructura de la organización.





## 1.2

# Ecosistema de una ciudad cibersegura

El ecosistema de la ciudad cibersegura está compuesto por:

- i) la ciudadanía** como destinataria de los servicios;
- ii) las plataformas y redes** de comunicaciones que permiten la entrega de información;
- iii) la infraestructura tecnológica** y los sistemas que dan sostén a la prestación de los servicios digitales ofrecidos y las actividades de las ciudades y municipalidades;
- iv) los dispositivos conectados**, las aplicaciones, los datos y la información que transmiten;
- v) un ecosistema urbano** a través del cual se prestan servicios públicos; y
- vi) la capacidad de ciberseguridad** para proteger sus activos, esto es, una instancia que involucra todos los elementos anteriores.

La infraestructura tecnológica, la provisión energética, la protección de los recursos, el suministro de servicios y el acceso a un buen gobierno son algunos de los principios que las ciudades y las municipalidades buscan cumplir de manera eficiente a través del uso de TIC. Dicha utilización por parte de la ciudad debe ser comprendida de manera integral, de tal forma que las garantías de ciberseguridad cubran cada uno de los frentes por los cuales los cibercriminales van a intentar buscar vulnerabilidades para así cumplir sus objetivos.

Gráfico 1.2.

## Ejemplos de elementos que se deben proteger



### Infraestructura de tecnologías

Redes wifi, ruteadores, dispositivos de conexión de redes, infraestructura de tecnologías de la información.



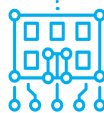
### Datos e información

Datos de seguridad, impuestos, movilidad, ambiente, ciudadanos.



### Sensores y dispositivos

Cámaras de vigilancia, teléfonos celulares, sensores de alumbrado, ambientales, de movilidad.



### Sistemas y APP

Sistemas financieros, de control y gestión, aplicaciones de los servicios de salud, movilidad.

Fuente: Elaboración propia (2021).





Figura 1.3.

# Ecosistema de una ciudad cibersegura

Fuente: Elaboración propia (2021).



## La ciudadanía

1



## Capacidad de ciberseguridad

6

## Ecosistema urbano

5





### 1.3

## Niveles estratégico, táctico y operativo de gestión de la ciberseguridad

La ciberseguridad debe ser gestionada desde el nivel estratégico del liderazgo de la ciudad, pasando por el nivel táctico de gestión de los secretarios y llegando al nivel operativo de los técnicos de ciberseguridad y de TIC.

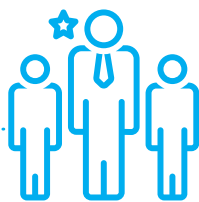
Gráfico 1.4.

## Niveles de gestión de la ciberseguridad



### ➤ **Estratégico**

**Le corresponde llevar la dirección general**, definir la visión, designar los recursos, asumir la responsabilidad y priorizar los objetivos de ciberseguridad para la ciudad, así como empoderar a los equipos técnicos para liderar y orientar las estrategias para alcanzar los objetivos. Aprueba la gobernanza, las normas, los lineamientos, las políticas y la gestión de recursos que estas demanden. Exige el cumplimiento de todos los roles.



### ➤ **Táctico**

**Le corresponde ejecutar las normas.** Garantiza que los equipos cumplan las normas, los lineamientos y las políticas, generalmente mediante la definición de planes, programas y proyectos alineados con las políticas priorizadas. Este es un nivel de planificación específico que profundiza los detalles para cada uno de los sectores (gobierno, movilidad, sanidad, etc.).



### ➤ **Operativo (técnico)**

**Propone las normas**, los lineamientos, las políticas, los estándares y los recursos necesarios para materializar los objetivos. Formula y ejecuta las estrategias, realiza el seguimiento y la supervisión de la ejecución. Entre otras tareas, propone las directrices técnicas y de capacitaciones; y los procedimientos para la gestión, identificación, protección, detección, respuesta y recuperación frente a incidentes (esta actividad la puede realizar personal vinculado directamente con la ciudad o municipalidad o terceros contratados).

Fuente: Elaboración propia (2021).



## 1.4

# Los ciberataques a las ciudades

Cuando un riesgo se materializa se está frente a un ciberataque a través del cual se lesionan o ponen en peligro, entre otros, los datos, la información, la infraestructura y, en general, cualquiera de los activos señalados en el numeral 1.1 de esta guía.

A continuación, se detallan los principales actores y motivos existentes para materializar un ciberataque; asimismo, se exponen los principales tipos de ataques y vulnerabilidades, y –por supuesto– los efectos que se observan cuando una ciudad o municipalidad se ve enfrentada a un ataque cibernético.

### 1.4.1

## Principales actores y motivos para materializar un ataque cibernético

Existen diversas motivaciones que influyen en la materialización de un ataque: cumplir un reto personal, obtener información empresarial o estatal privilegiada, buscar un objetivo político u obtener un valor económico. Estos motivos no son excluyentes entre sí; por el contrario, en un ciberataque pueden coexistir: por ejemplo, puede cometerse una actividad criminal de espionaje con fines empresariales o políticos.

Cualquiera de estos motivos sirve de fundamento para colocar a las municipalidades en riesgo. Estos motivos pueden estar en cabeza de uno o de varios actores, como se verá a continuación.

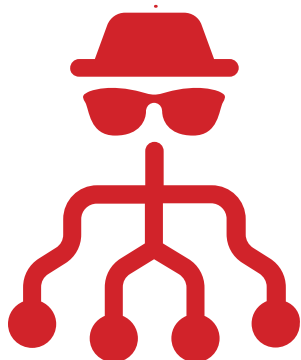


Figura 1.5.

## Motivos para materializar un ataque cibernético en una ciudad



### Personales

El atacante quiere satisfacer un deseo, una necesidad o cualquier otra cuestión vinculada consigo mismo. La superación personal, cumplir un reto, la curiosidad, la venganza, la satisfacción personal, entre otros, pueden constituir un motivo para cometer un ataque cibernético.



### Criminales

La motivación criminal puede estar vinculada a dos finalidades. Por un lado, al daño, lesión o puesta en peligro de los bienes jurídicos de la víctima; por otro, a la obtención de un provecho para el victimario o para un tercero.



### Empresariales

La puesta en peligro de la información, la obtención de secretos corporativos, el conocimiento de la actividad empresarial, de la infraestructura que da soporte a los servicios y, en general, de los bienes o servicios ofrecidos, pueden convertirse en motivos para la materialización de un ataque informático.



### Políticos

La motivación criminal puede estar asociada a la modificación del régimen político imperante, la caída de un sector democrático, el direccionamiento para la toma de una decisión ciudadana, la puesta en peligro o desestabilización de la soberanía, el gobierno, el territorio o la población de una nación.



### Económicos

La materialización de un ataque puede buscar una retribución, una compensación, un beneficio o una ganancia para el atacante o para un tercero.



### Otros

Existen otras motivaciones. Además, puede haber motivos que se complementen unos con otros. Un ejemplo puede ser la realización de una actividad criminal por venganza que, al mismo tiempo, tenga un motivo empresarial o económico.

Fuente: Elaboración propia (2021).

Cuando se produce un ciberataque hay una serie de actores, víctimas y victimarios. El papel que cada actor desempeña se detalla en el gráfico 1.6.

Gráfico 1.6.

## Principales actores de los ciberataques



### Activos




Quienes realizan el ataque cibernético de manera directa o indirecta:

-  **Ciber**criminales
-  **Ciber**espías
-  **Ciber**terroristas
-  **Ciber**activistas



### Pasivos

Víctimas del ataque cibernético:

-  **Ciudadanos**
-  **Empresas y** organizaciones privadas
-  **Estados** o cualquier autoridad pública (por ejemplo, municipalidades)

Cualquiera sea el tipo de actores (activos o pasivos):



**Públicos**

**Privados**

**Nacionales**

**Extranjeros**

**Individuales**

**Colectivos**

Fuente: Elaboración propia (2021).

Desde cada uno de los papeles que cumplen los diversos actores, deben comprenderse los tipos de amenazas a los que puede estar sometido el gran ecosistema urbano.





#### 1.4.2

### Principales tipos de ataques y vulnerabilidades

Los objetos de un ciberataque pueden ser la información, el *hardware*, el *software*, los servicios ofrecidos, las redes y conexiones, los recursos humanos, la infraestructura crítica cibernética y, en general, cualquier activo o servicio de la ciudad que utilice TIC. Los ataques más frecuentes están vinculados al uso de ingeniería social, programas malignos, fuerza bruta para obtener el acceso y ataques a las conexiones e infraestructura. Dichas acciones buscan, entre otras metas, atentar contra la privacidad, integridad o disponibilidad de los sistemas de información y, en general, saltar las medidas de seguridad.



Las autoridades urbanas y municipales deben conocer las técnicas más frecuentes (también llamadas técnicas de *hacking*) y los principales tipos de amenazas. El gráfico 1.7 sintetiza algunas de ellas.

Gráfico 1.7.

## Tipos de amenazas y ataques



### Ransomware

Actividad a través de la cual se toma control del dispositivo y se encripta la información; en algunos casos se exfiltra la misma bajo amenaza de publicación. A cambio de recuperar el control y la información, se exige el pago de un rescate.



### Ataques de denegación distribuida de servicio (DDoS)

Acometida a un servidor o red al mismo tiempo desde muchos equipos diferentes con redes zombis para que deje de funcionar al no poder soportar tantas peticiones.



### Redes trampa (wifis falsas)

Creación de una red wifi gemela a otra legítima y segura, con un nombre igual o muy similar a la original para robar los datos de quienes se conecten a ella.



### Phishing

Envío de mensajes mediante una identidad que parece ser legítima, para lograr el objetivo de intrusión y ataque.



### Mail spoofing / suplantación de origen de correo electrónico

Uso de la dirección de correo de una persona o entidad de confianza para conseguir información personal que se transmite bajo engaño.



### Zombis / botnet

Un número de distintos dispositivos infectados y a su vez controlados por los ciberdelincuentes.



### Ingeniería social

Conjunto de técnicas dirigidas a manipular psicológicamente a los usuarios para que tomen una acción comprometedora, por ejemplo, mediante la revelación de información personal o la navegación de páginas maliciosas, lo que permite tomar el control de los dispositivos.



### Inyección SQL

Ataque a un servicio web basado en este tipo de lenguaje, comprometiendo la base de datos mediante líneas de código malicioso y aprovechando vulnerabilidades en su programación.



### Spam o correo no deseado

Envío de grandes cantidades de mensajes o de mensajes publicitarios a través de Internet sin que hayan sido solicitados.



### Troyanos

Virus para controlar un equipo, robar los datos, introducir más *software* malicioso en el equipo y propagarse a otros dispositivos.



### Anuncios maliciosos

Buscan recopilar información de la actividad del usuario y, de este modo, mostrar anuncios dirigidos. Su instalación puede suponer una baja de rendimiento y un mal funcionamiento del dispositivo.



### “Man in the middle”

Conocido como ataque de intermediario. Aquí el intermediario malicioso se ubica entre dos activos que se están comunicando e intercepta la comunicación; de este modo, gana acceso para leer o manipular los datos, mensajes, credenciales o transferencias que se intercambien.

Fuente: Elaboración propia (2021).



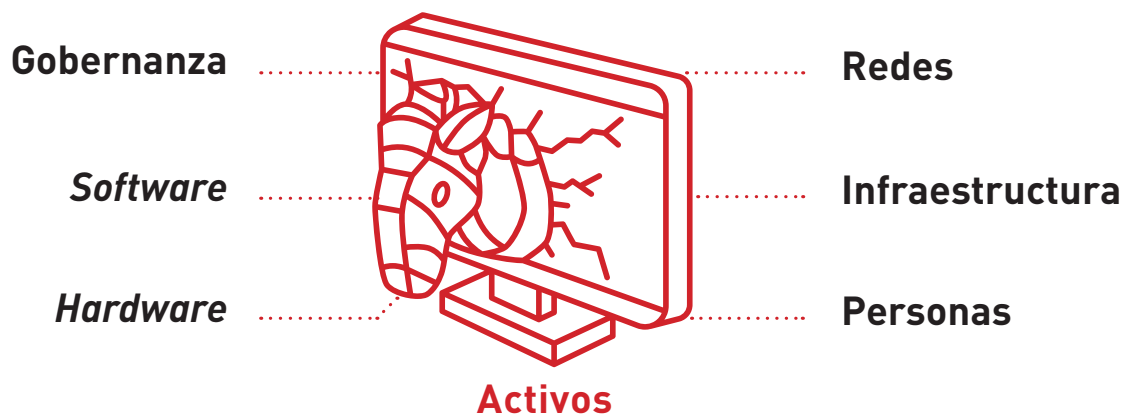
También existen otras técnicas o métodos de ataque, como el analizador de datos, las aplicaciones maliciosas, ataques a *cookies*, envenenamiento de la caché de DNS, suplantación de direcciones IP, escaneo de puertos, falso antivirus, gusanos, puertas traseras, registrador de teclas, *software* espía, suplantación de una página web, secuestro de información confidencial, ataques ciberfísicos y criptominería, entre otros. Todas estas acciones se pueden combinar unas con otras y sus resultados pueden ser devastadores.

Los ataques cibernéticos tienen cabida porque hay vulnerabilidades, esto es, fallas en los activos (*software*, *hardware*, redes, infraestructura), la interacción entre los activos o la gobernanza. Además, el **factor humano** presenta una de las principales debilidades de las que se aprovechan los ciberdelincuentes para conseguir sus objetivos. Pueden tener su origen dentro de las organizaciones o fuera de estas, a través de las cadenas de suministro y demás terceros (clientes, autoridades de control, etc.).

Por ello, es imprescindible la implementación de controles de manera permanente, la identificación de vulnerabilidades, la formación constante, la colaboración entre los actores y la gestión adecuada de los riesgos y de los incidentes, los cuales constituyen las principales actividades para proteger los activos de la organización.

Gráfico 1.8.

## Origen de las principales fallas y vulnerabilidades



Fuente: Elaboración propia (2021).





Entre otros elementos, los cibercriminales se aprovechan de las fallas y vulnerabilidades que se presentan en las ciudades, vinculadas a los siguientes defectos:

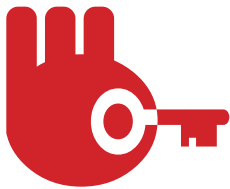
- 1. Ausencia de una estrategia de ciberseguridad integral.
- 2. Falta de gobernanza, normas, lineamientos y políticas de ciberseguridad.
- 3. Falta de integración completa de la cadena de suministro y de terceros que se relacionan con la ciudad en el proceso de ciberseguridad.
- 4. Inexistencia de una política de protección de datos.
- 5. Falta de una adecuada gestión de las vulnerabilidades, los riesgos y los incidentes.
- 6. Falta de actualización del *software* y *hardware* dispuestos para la prestación de los servicios de la ciudad.
- 7. Fallas en el *software* y *hardware* dispuestos.
- 8. Falta de capacitación y formación del personal y demás intervinientes (terceros, usuarios).
- 9. Falta de recursos económicos para desarrollar la estrategia de ciberseguridad de la ciudad.
- 10. Falta de cooperación y colaboración entre las distintas autoridades y el sector privado.
- 11. Ausencia de capacidades (recursos humanos, herramientas, tecnologías).
- 12. Falta de comprensión del entorno digital.
- 13. Inexistente o errónea aplicación de controles técnicos.

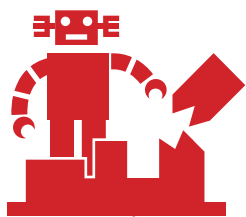
### 1.4.3

## Consecuencias que puede generar un ataque informático a la ciudad

Los riesgos materializados a través de los ataques generan consecuencias como las siguientes:

- **Interrupción de servicios críticos** de la ciudad, como energía, suministro/tratamiento de agua, movilidad, salud, control de tráfico, etc.
- **Reducción de la productividad** de los trabajadores.
- **Suspensión de la recaudación** de ingresos propios municipales.
- **Imposibilidad de prestar servicios** al ciudadano, como la realización de trámites o el despacho de autorizaciones, entre otros.
- **Daño a la reputación** de la administración municipal y desconfianza.
- **Violación de las leyes** de privacidad y confidencialidad de datos, lo cual puede generar investigaciones y sanciones.
- **Pérdida de las inversiones** que se han realizado para la prestación de servicios.
- **Desestabilización política, económica, o social.**
- **Afectaciones a la integridad, disponibilidad, confidencialidad y autenticidad de los datos.**





## 1.5

# Ataques informáticos que han paralizado ciudades

De acuerdo con la taxonomía de los daños cibernéticos planteada por Agrafiotis (2018), estos comprenden cinco clases generales: i) daño físico o digital, ii) daño económico, iii) daño psicológico, iv) daño a la reputación y v) daño social. Estos daños pueden estar conectados y, en función del ataque, puede haber una mayor o menor propagación. Diariamente se producen cientos de miles de ciberataques, muchos de ellos a ciudades y otro tipo de infraestructura crítica.<sup>2</sup> Afortunadamente, la inmensa mayoría no tiene relevancia, precisamente, gracias a la ciberseguridad. Desde 2003, ha habido casi 1.000 ciberataques, que han generado costes de más de US\$1 millón (CSIS, 2021) cada uno, y más de 500 secuestros de datos relevantes en 2020 y 2021.<sup>3</sup>

Pese a los años transcurridos, el **ciberataque a Estonia ocurrido en abril de 2007 supuso un punto de inflexión para que los poderes públicos y las ciudades comenzaran a tomar en serio la ciberseguridad**. Tras una polémica retirada de una estatua se produjo una avalancha de solicitudes de acceso (DDOS) que bloqueó la red de Internet del país e impidió el acceso a servidores, bancos, periódicos y a numerosos servicios electrónicos del gobierno. Para el ataque, se utilizaron más de un millón de computadoras que, por haber accedido a un correo o a una página, descargaron un *software* malicioso que las convirtió en zombis controlados a distancia para conectarse a un mismo punto a fin de colapsarlo. Del lado positivo, **la situación llegó a la Organización del Tratado del Atlántico Norte (OTAN) y se inició el camino de la ciberseguridad en la Unión Europea y en instituciones internacionales**. Asimismo, desde entonces el gobierno de Estonia comprendió la importancia de una estrategia de ciberseguridad, de la necesidad del impulso público y de la colaboración entre el Estado, la industria y el ámbito académico. **Estonia pasó a ser uno de los países más avanzados a nivel digital de todo el mundo**, en buena medida como reacción a este ataque. En este caso los daños fueron sociales, digitales y económicos.

2. Véanse las páginas: <https://www.sicherheitstacho.eu/start/main>, <https://cybermap.kaspersky.com/es>, <https://www.fireeye.com/cyber-map/threat-map.html>, <https://horizon.netsecout.com>.

3. Véase <https://cloudian.com/ransomware-attack-list-and-alerts>.





**Entre los ciberataques destacados de los últimos años, cabe recordar que su objetivo han sido los sistemas policial, de emergencia o de transporte de las ciudades.** En abril de 2021 los ciberatacantes extrajeron más de 250 GB de información muy sensible del Departamento de Policía de **Washington, D.C.** Como prueba de ello, difundieron parte de la información, reclamaron dinero y amenazaron con “contactar bandas para purgar a los confidentes” (de la policía). El protagonista de esta ocasión fue un secuestro de datos informáticos (*ransomware*). Se trata de un ataque que sigue la línea marcada ya en junio de 2017, cuando los *hackers* consiguieron encender las sirenas de alerta de tormentas, desastres, etc. de la población estadounidense de **Dallas**, Texas, lo que ocasionó que las líneas de emergencia colapsaran. En enero de 2017, y durante cuatro días, actores criminales habían tomado el control de las cámaras de seguridad del Departamento de Policía Metropolitana del Distrito de Columbia (MPDC). En noviembre de 2017, el Sistema Regional de Transito de Sacramento, Estados Unidos, recibió un ciberataque cuyo resultado final fue la pérdida de información de programas y datos necesarios para el despacho de autobuses y la planificación de rutas.



**El sistema de salud ha sido también un objetivo importante, lo que ha resultado costoso.** En efecto, en enero de 2020, un ciberataque al Hospital Universitario de Torrejón, en **Madrid**, España, dañó varios de los sistemas informáticos (daños digitales). Esta línea había sido trazada algunos años atrás y tiene como antecedente para resaltar el mes de mayo de 2017, cuando la red hospitalaria de Londres sufrió un *ransomware* que afectó a hospitales, centros de salud y pacientes, entre otros. La red de ambulancias se vio perjudicada, el personal médico no pudo acceder a las historias clínicas de los pacientes y se puso en peligro la vida de los ciudadanos; se anularon miles de citas y se reubicaron pacientes de emergencia. Se estima que esto ha tenido un costo de £92 millones (US\$130 millones).<sup>4</sup>



**Atlanta, Estados Unidos: una ciudad colapsada y un gobierno que dimite por no invertir a tiempo en ciberseguridad.** En marzo de 2018 los atacantes lograron romper contraseñas por la fuerza en Atlanta. Ello afectó durante semanas a muchos servicios y programas de la ciudad, incluidos los estacionamientos y servicios judiciales. Los funcionarios de la ciudad se vieron obligados a completar formularios a mano en papel. Hay que destacar que antes del ataque el gobierno de Atlanta había sido criticado por su escaso gasto y fallas en ciberseguridad. No invertir a tiempo tuvo un enorme coste político y económico posterior. Así, la situación trajo aparejada la dimisión de docenas de funcionarios y de todo el gabinete. Atlanta debió invertir US\$2,7 millones para recuperarse.

4. Véase <https://www.acronis.com/en-us/articles/nhs-cyber-attack>.



Colin Lloyd



Colonial Pipeline

El secuestro de la **ciudad de Baltimore (Maryland, Estados Unidos)** fue ciertamente una pesadilla. En mayo de 2019 un *ransomware* bloqueó computadoras, sistemas y correos electrónicos, entre otros activos de la alcaldía. Se solicitó al gobierno que pagara 13 *bitcoins* (aproximadamente US\$76.280), pero el alcalde se negó.<sup>5</sup> Se estima que esa decisión generó un costo de US\$18,2 millones. La ciudad no funcionó con normalidad en tres semanas y se necesitaron meses para lograr la recuperación.

En agosto de 2021, los datos de la **Alcaldía de Santa Fe de Antioquia, Colombia**, fueron secuestrados y utilizados con fines extorsivos. Como consecuencia, los ciudadanos no pudieron realizar trámites virtuales y se dispuso congelar las cuentas municipales. Asimismo, en marzo de 2021 el **Servicio Público de Empleo Estatal (SEPE) de España** fue objeto de un ataque por el *ransomware* Ryuk, lo que dificultó y retrasó durante tres semanas la gestión del pago de subsidios de desempleo. En este caso, se resaltó el hecho de que los sistemas informáticos no estaban suficientemente actualizados, lo cual posibilitó el ataque. En mayo de 2021, el **gobierno de Estados Unidos** decretó el estado de emergencia regional por un ciberataque de *ransomware* a los sistemas de **Colonial Pipeline**, la mayor red de oleoductos del país. El ataque logró desconectar la infraestructura tecnológica del oleoducto que se extiende por más de 5.500 millas entre Texas y Nueva Jersey, y representa el 45% del diésel, la gasolina y el combustible que consumen los aviones de la Costa Este del país. Fue un secuestro a cambio del cual se solicitaba dinero.

En diciembre de 2019 el gobierno de la **provincia de San Luis, Argentina**, tuvo que declarar la emergencia durante 90 días; su sistema de expedientes fue secuestrado con demanda de dinero. Al parecer, la ciudad no pagó y se logró recuperar la información hasta diciembre de 2018, pero se presentaron importantes problemas para descifrar los 350 GB correspondientes a todo 2019. Por su parte, en febrero de 2020 la **Secretaría de Economía de México** tuvo que suspender plazos administrativos luego de que quedaran afectados expedientes y correos electrónicos tras un ataque.

5. Disponible en <https://twitter.com/mayorbcyoun/status/1136377418325864448>.

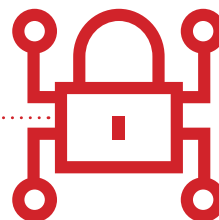


En junio de 2021 la **Universidad del Bosque de la ciudad de Bogotá** comunicó a toda la comunidad académica que había sido víctima de un ciberataque de seguridad, por el cual algunos de sus sistemas internos quedaron comprometidos. Presuntamente, dicho ataque tuvo lugar a través de una denegación de servicios distribuida y trajo como resultado el bloqueo de las actividades administrativas y académicas por varios días.

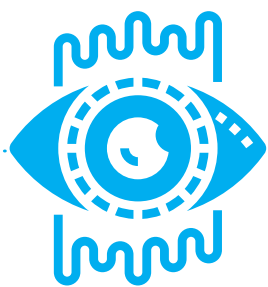
**Una historia con final feliz gracias a la previsión. En junio de 2021 la red de metro de la ciudad de Nueva York** sufrió un ataque informático. La Autoridad de Tránsito Metropolitano (MTA) contaba con una estrategia de ciberseguridad robusta, lo que le permitió contener el ataque y mantener la prestación de sus servicios. Al parecer, la planificación y las múltiples capas existentes de la MTA funcionaron según lo diseñado. Además, en los últimos meses, se había desarrollado una sensibilidad especial, junto con elementos de previsión, tras diversos ataques ocurridos contra infraestructura crítica de Estados Unidos.



**Con la COVID-19 comenzaron nuevas formas de ciberataques.** La ingeniería social, la extrema necesidad de suministros esenciales y la información relacionada con la COVID-19 empezaron a utilizarse como señuelos para la obtención de datos, la realización de estafas y el *phishing*, y se secuestraron computadoras a través de *malware*, adjuntos malignos y suplantación de la identidad. También hubo ataques *ransomware* y DDoS contra hospitales y centros médicos desbordados. Del mismo modo, se explotó la vulnerabilidad del trabajo a domicilio para robar datos, obtener ganancias o provocar disfunciones (Interpol, 2020). Así, por ejemplo, en marzo de 2020, en **Costa Rica**, una aplicación de *ransomware* llamada COVIDLock se extendió por todo el país y afectó también al sector público. La aplicación teóricamente facilitaba mapas interactivos de la propagación del virus, y aprovechaba el interés de los usuarios para secuestrar los dispositivos y reclamar *bitcoins* (daños económicos y sociales).







## 1.6

# La madurez en ciberseguridad de las ciudades inteligentes

Como se concluye desde el Instituto Nacional de Estándares y Tecnología (NIST)<sup>6</sup> (NIST, 2019), las ciudades y comunidades inteligentes no son sostenibles ni verdaderamente inteligentes si no identifican, despliegan y mantienen de forma proactiva y adaptativa los procesos y medidas de gestión de riesgos de ciberseguridad y privacidad. Ello, además, genera confianza y facilita la participación en la ciudad inteligente.

En su medida 7, la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) (ENISA, 2015) señala que las ciudades inteligentes y los organismos de normalización deben integrar la ciberseguridad en el nivel de madurez urbana. Así, las ciudades más maduras podrán compartir sus medidas de seguridad como ejemplo, y las menos maduras, además de aprender, tendrán estímulos para la mejora.

Sin embargo, no hay suficiente concienciación. Los más destacados *rankings* internacionales de madurez digital de las ciudades no contemplan la ciberseguridad: IMD-SUTD Smart City Index (SCI),<sup>7</sup> Top 50 Smart City Government Rankings (smartcitygovt),<sup>8</sup> Smart City Winners, IESE's Top 10 By Dimension,<sup>9</sup> JUNIPER Research 2019-2023,<sup>10</sup> etc.

**Una mejora para la situación.** El BID ha empezado a integrar la seguridad y la privacidad, por un lado, en sus cinco niveles que sirven para medir el grado de madurez de la *smart city* (Townsend y Zambrano-Barragán, 2019: 19 y ss.). Por otro lado, la seguridad y la privacidad constituyen una de las cuatro dimensiones del diagnóstico de madurez de *Big Data* para el desarrollo urbano (Biderman et al., 2021). Recientemente, la hoja de ruta para las “ciudades pioneras” del G-20 integra la seguridad y la privacidad como elemento esencial (Alianza Global de Ciudades Inteligentes del G-20, 2021). Y en Japón (MIAC, 2020) la privacidad y la seguridad también son elementos básicos.

6. El Instituto Nacional de Estándares y Tecnología (NIST) depende del Departamento de Comercio de Estados Unidos. El Marco de Ciberseguridad del NIST ayuda a los negocios de todo tamaño a comprender mejor sus riesgos de ciberseguridad, a administrar y reducir sus riesgos, y a proteger sus redes y datos.

7. Véase <https://www.imd.org/smart-city-observatory/smart-city-index>.

8. Véase <https://www.smartcitygovt.com>.

9. Véase <https://smartcity.press/top-10-smart-cities-of-2020>.

10. Véase <https://www.juniperresearch.com/researchstore/key-vertical-markets/smart-cities-research-report/subscription/leading-platforms-segment-analysis-forecasts>.

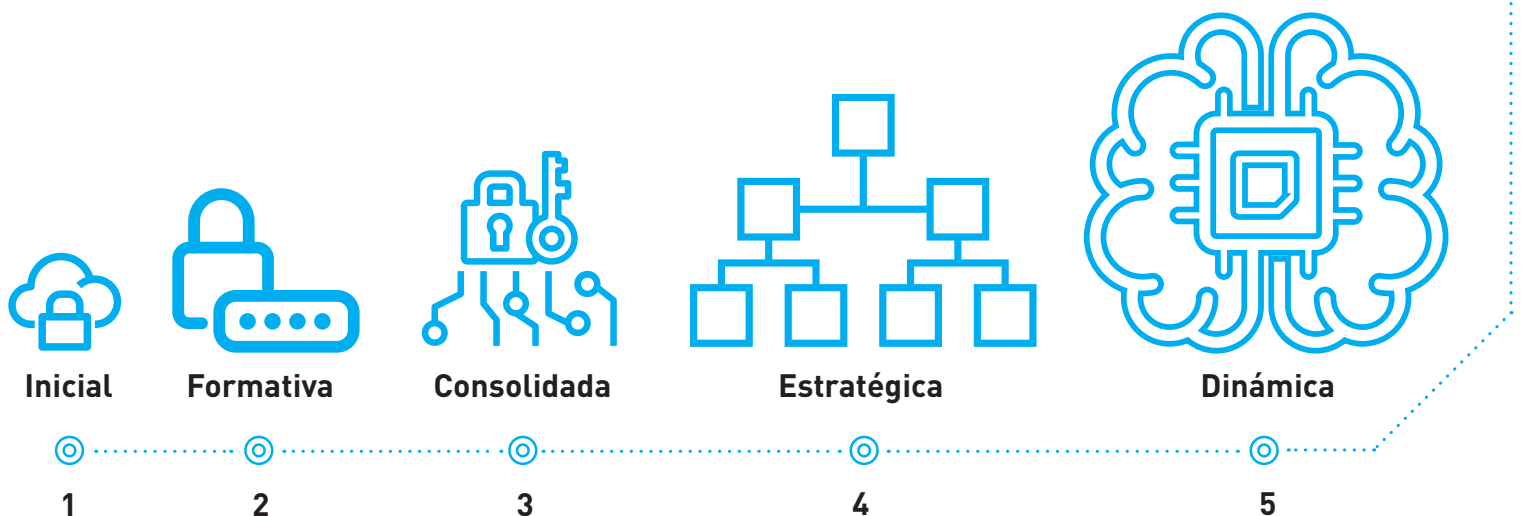


La Alianza Global de Ciudades Inteligentes del G-20 sobre Gobernanza Tecnológica, que reúne a los gobiernos municipales, regionales y nacionales, a los socios del sector privado y la sociedad civil, fue creada en 2019 para recopilar y analizar políticas para ciudades inteligentes y éticas exitosas. Ya se cuenta con una política modelo de gobernanza (Alianza Global de Ciudades Inteligentes del G-20, 2020) y una hoja de ruta (FEM, 2021), dentro de la que se ha incorporado la ciberseguridad como elemento transversal.

En ALC recién a partir de 2016 se ha suscitado un mayor interés por crear seguridad en el entorno digital para los países. Mediante un trabajo conjunto del BID y de la OEA (BID y OEA, 2020), se aplicó en América Latina y el Caribe el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM, por sus siglas en inglés). Este modelo, elaborado por el Centro Global de Capacidad en Seguridad Cibernética de la Universidad de Oxford, evalúa el nivel de madurez de las capacidades de ciberseguridad de un país en cinco etapas: 1) Inicial; 2) Formativa; 3) Consolidada; 4) Estratégica y 5) Dinámica.

Gráfico 1.9.

## Las cinco etapas de madurez de la capacidad de ciberseguridad

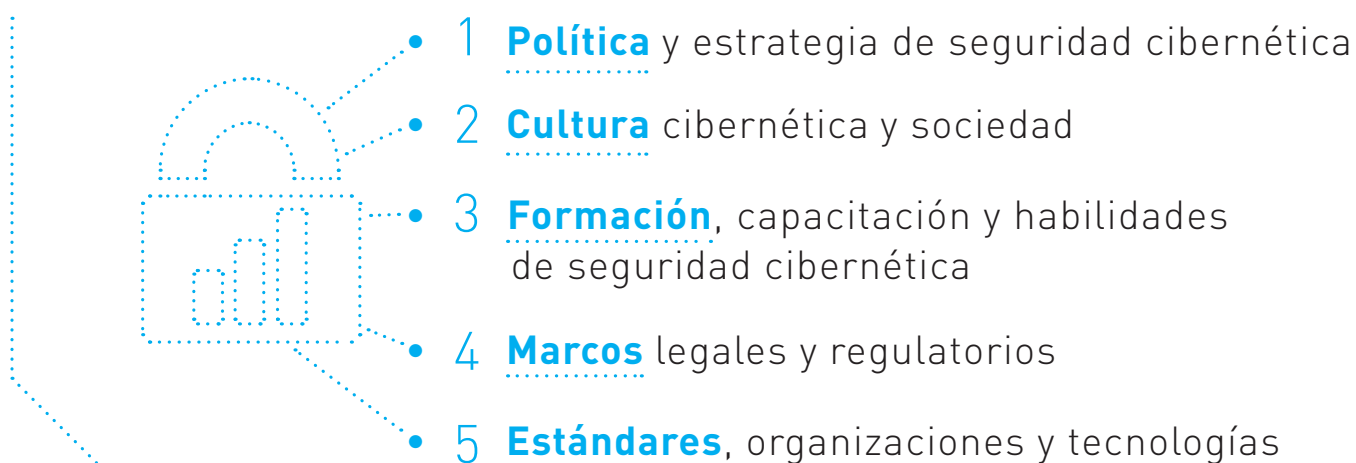


Fuente: BID y OEA (2020: 42).

A su vez, la evaluación de los niveles de madurez se divide en cinco dimensiones: 1) Política y estrategia de ciberseguridad; 2) Cultura cibernética y sociedad; 3) Educación, capacitación y habilidades en ciberseguridad; 4) Marcos legales y regulatorios; y 5) Estándares, organizaciones y tecnologías. Estos se subdividen en un conjunto de factores que describen y definen lo que significa poseer capacidad de seguridad cibernética en cada factor e indican cómo mejorar la madurez. Los indicadores y el modelo son también de utilidad y sirven de referencia para las ciudades.

Gráfico 1.10.

## Las cinco dimensiones del Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones



Fuente: Elaboración propia (2021).

Dentro de los hallazgos principales de los reportes (2016, 2020) se detecta un aumento significativo del interés y de la conciencia en ciberseguridad, así como un incremento sustancial de la madurez en este campo, lo cual incluye una mayor capacidad de los organismos rectores, la elaboración de estrategias nacionales y legislación. Los países de la región han emprendido el camino hacia la transformación digital con ciberseguridad y el reto es que las ciudades logren implantar muchos de los elementos que se presentan en estos reportes.

En el proceso de migración hacia una *smart city* y en el uso de *Big Data* urbano, es fundamental que se incorporen capacidades que permitan contar con un nivel de ciberseguridad adecuado. Asimismo, se debe establecer como prioridad la implementación de la función de ciberseguridad, de tal manera que los servicios ofrecidos en la ciudad sean seguros.







# 2

## *Recomendaciones y recursos para proteger las ciudades de los ciberataques*

Daniel Lloyd Blunk Fernández

*«La arquitectura e infraestructura tecnológica de la ciudad es compleja; los actores que intervienen son muy variados; también lo son la información y los datos que se deben proteger.»*

# 2

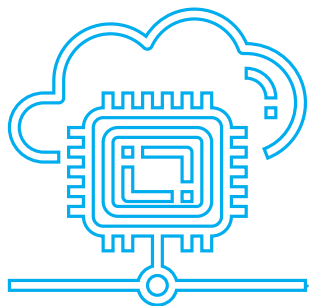
## Recomendaciones y recursos para proteger las ciudades de los ciberataques



El lector o la lectora de esta guía ya conocen el concepto de ciberseguridad y de las ciberamenazas que ponen en jaque a las ciudades en el ciberespacio. La respuesta para proteger las ciudades de los ciberataques consiste en implementar acciones proactivas para fortalecer la ciberseguridad. Hace unos años, el BID (Bouskela et al., 2016: 115) publicó *La ruta hacia las Smart Cities*. Ahora propone una hoja de ruta hacia la ciberseguridad de las ciudades. El gráfico 2.1 contiene dicha hoja de ruta con las recomendaciones, las prácticas y los recursos necesarios para proteger cualquier tipo de ciudad con un enfoque basado en la gestión del riesgo.

Gráfico 2.1.

### Hoja de ruta hacia la ciberseguridad urbana



1. **Identificar** los activos y actores que se van a proteger
2. **Establecer** la gobernanza de la ciberseguridad
3. **Institucionalizar** la ciberseguridad
4. **Integrar** la seguridad de los datos confidenciales de la ciudad y los datos personales
5. **Integrar** los proveedores a la ciberseguridad
6. **Formar**, comunicar y concientizar acerca de la ciberseguridad
7. **Disponer** de financiamiento y seguros para ciberseguridad

Fuente: Elaboración propia (2021).



La **arquitectura e infraestructura** tecnológica de la ciudad es compleja; los **actores** que intervienen son muy variados; también lo son **la información y los datos** que se deben proteger. Por eso, el primer paso es la identificación de todos estos elementos (NIST, 2019), lo cual debe estar esencialmente a cargo del personal táctico y tecnológico de la ciudad.

A partir del conocimiento de la complejidad de la ciudad que se va a proteger y de los sujetos, el nivel estratégico debe establecer una **gobernanza** que integre de manera global la gestión de la ciberseguridad, de la ciudad inteligente y del dato. Como premisa, hay que tener en cuenta las leyes y normas de seguimiento obligatorio, para lo cual el nivel táctico constituye un apoyo fundamental. Asimismo, especialmente desde los perfiles tecnológicos, hay que elegir entre diversos esquemas de estandarización y certificación de ciberseguridad. Sobre estas bases, se recomienda que el nivel estratégico fije para la ciudad políticas y normas de seguridad comunes, con competencias claras y con participación de las partes. Asimismo, la ciberseguridad urbana debe conectarse con las políticas nacionales. El establecimiento de una gobernanza conlleva la **institucionalización** a cargo del nivel estratégico. Se debe designar un responsable de ciberseguridad, con las funciones concretas que se señalan aquí. En estas páginas también se puntualizan buenas prácticas para conseguir que los niveles tácticos y tecnológicos compartan información de seguridad.

**Hay que proteger la información y los datos.** Por lo general bajo parámetros legales, el nivel táctico identifica si hay datos confidenciales y personales para proteger especialmente y el nivel tecnológico implanta la protección correspondiente. Entre las mejores prácticas al respecto, se subraya la de anonimizar (y seudonimizar) y cifrar los datos que maneja la ciudad.

Del mismo modo, se recomienda **integrar en la ciberseguridad la elección, gestión y contratación de proveedores y prestadores de servicios**, labor para la cual el personal de nivel táctico es esencial. Asimismo, entre las recomendaciones y buenas prácticas más destacadas, cabe mencionar **la cultura de ciberseguridad, la concienciación y la formación** de los responsables y del personal de la ciudad. Finalmente, resulta fundamental contar con presupuesto para ciberseguridad y valorar la contratación de seguros. Para ello, se precisa el impulso del nivel estratégico, junto con el apoyo táctico.



Daria Nepriakhina





## 2.1

# Identificar los activos y actores que se van a proteger

Hoy en día, la prestación de servicios y la gestión de la infraestructura urbana a través de las TIC es esencial para una ciudad. Sin embargo, su empleo implica gestionar los riesgos que esto conlleva. Como se ha señalado en el apartado anterior, muchas ciudades han visto paralizada la prestación de los servicios debido a múltiples ataques informáticos.

Para empezar, **se debe identificar qué se va a proteger**, esto es, **los activos principales (procesos y actividades de negocios y datos críticos)** y los activos de apoyo de esa información (**hardware, software, red, personal, estructura de la organización**, etc.), a los que se ha de brindar seguridad, y medir el nivel de impacto posible frente a un ciberataque.

Hay que tomar conciencia de todos los elementos inteligentes que se apoyan en el ciberespacio y que no están protegidos: sistemas industriales inteligentes (redes SCADA), por ejemplo, los sistemas de distribución eléctrica; los sistemas de vigilancia de la ciudad; los sistemas de sensores de variables ambientales que se sustentan en el Internet de las cosas (IIoT). La presencia de estos dispositivos hace que el perímetro por proteger se vuelva prácticamente ilimitado. En el ecosistema de la ciudad, además de las tecnologías del IoT más habituales, acaban coincidiendo numerosas tecnologías heterogéneas, protocolos de comunicaciones diversos, mecanismos ciberfísicos (controlados por algoritmos e integrados con Internet), robots, drones y vehículos autónomos. Y todo en consonancia con tecnologías conexas de nube, *Big Data*, inteligencia artificial. Por otra parte, es esencial identificar y considerar las interdependencias entre sistemas, puesto que un sistema de bajo riesgo puede estar vinculado a otros o, por el contexto, puede ser de alto riesgo. Asimismo, de acuerdo con ENISA (2015), se debe tomar en cuenta el problema que implican los largos ciclos de vida de los equipos utilizados o los sistemas heredados, que rara vez cumplen con la seguridad en el diseño. Ello debe resolverse a través de un plan de inversión (OSPI, 2017: 8).

**Se debe trazar un mapa que integre la gran diversidad de actores públicos y privados que interactúan y a los que hay que orquestar y dotar de gobernanza:**



- Altos directivos.
- Sectores de la ciudad más especializados en el ámbito tecnológico, de ciberseguridad y protección de datos.
- Áreas competentes en seguridad (seguridad policial, laboral, etc.).
- Áreas sectoriales más implicadas con la digitalización (finanzas, transporte, residuos, salud, suministros, etc.).
- Superestructuras de cooperación o de coordinación creadas a nivel local, regional o nacional.
- Responsables de las diversas capas de servicios, infraestructura, comunicaciones, etc., que suelen ser prestadores de servicios y comunicaciones a terceros y, por lo general, privados (agua, luz, movilidad y transporte, seguridad, etc.).
- Entidades del sector público que en ocasiones son a su vez prestadoras y proveedoras de servicios a la ciudad.
- Tercer sector, organizaciones no gubernamentales (ONG) o el ámbito académico, que pueden integrarse en procesos de análisis o participación (Muñoz et al., 2016: 26).
- Ciudadanía, que es destinataria de servicios y, a la vez, constituye el grupo al que pertenecen los datos que alimentan la ciudad, y es la que sufre los ataques que pudieran ocurrir o las fallas en los servicios.





## 2.2

# Establecer la gobernanza de la ciberseguridad

A partir de la identificación de los activos, datos y procesos que se deben proteger y de los actores que se deben orquestar, hay que establecer un esquema de gobernanza clara de la ciberseguridad.

### 2.2.1

## Establecer la gobernanza de la ciberseguridad e integrarla en la gobernanza de la ciudad

**La gobernanza de la ciberseguridad se integra en la gobernanza de la ciudad inteligente, la cual implica la creación de normas y políticas, así como la construcción de una estructura organizativa** (MIAC, 2020). Según el Foro Económico Mundial (FEM) (FEM, 2021), la gobernanza de la *smart city* supone la integración de cinco políticas:

1. **Accesibilidad**, inclusión e impacto social.
2. **Seguridad** y resiliencia.
3. **Privacidad** y transparencia.
4. **Apertura** e interoperabilidad.
5. **Política** de datos abiertos y políticas de *Dig Once* para garantizar que la infraestructura digital se instale con sostenibilidad operativa y financiera.

La dirección y gestión de la ciudad y la ciudad inteligente pueden verse como el tratamiento y la explotación masiva de ingentes cantidades de datos. Y la gobernanza de la ciudad –y su ciberseguridad– debe integrarse en **la más amplia gobernanza del dato**. Ello implica, entre otras acciones, **fijar las fuentes de datos, su ordenamiento y tráfico, las instituciones y órganos, las competencias y responsabilidades, las pautas de gestión**. Es menester identificar los datos necesarios y las fuentes de los que proceden y determinar dónde integrar, recopilar, depurar y ordenar los datos, analizarlos e interpretarlos.

La gobernanza de la ciberseguridad debe incluir la gobernanza del dato y ello supone establecer responsabilidades en cuanto a la toma de decisiones sobre actualización, acceso, disponibilidad, propiedad,





seguridad, privacidad. De igual modo, implica fijar las pautas y normas de su gestión, su calidad y sus usos. La gobernanza requiere gestionar la arquitectura y la infraestructura de datos, así como la interoperabilidad y los protocolos para facilitar el intercambio de datos, tanto de forma interna como externa, con otras administraciones o con entidades privadas. La gobernanza del dato también permite redefinir las competencias profesionales y la gestión de recursos humanos, y atraer o incorporar los perfiles adecuados. Asimismo, posibilita la transformación del modelo de gestión y propicia un cambio cultural para todo el ecosistema.

Para la innovación y la *smart city*, el BID ha subrayado **la importancia de designar liderazgos**, que generan cultura de gobernanza de datos, así como de establecer autoridades democráticas para la innovación (Townsend y Zambrano-Barragán, 2019: 41). **Con la creación de órganos de gobernanza o su regulación se lanza un mensaje explícito de la importancia de este punto.** Asimismo, se puede generar una dinámica de centralización de criterios y metodologías de recopilación, tratamiento y explotación de datos y de impulsar repositorios de datos compartidos. Al mismo tiempo, esto permite descentralizar acciones específicas respecto de los distintos sectores, lo cual facilita la coordinación y la interoperabilidad, y propicia dinámicas transversales (Salvador, 2021).

### Ejemplos para seguir sobre gobernanza del dato:

- **La creación de órganos: la Mayor's Office of Data Analytics (MODA) de Nueva York y la Citywide Analytics Team de Boston, creadas en 2015; la London Office of Data Analytics (LODA) de 2017. En España, la Oficina Municipal de Datos (OMD) del Ayuntamiento de Barcelona, instaurada en 2018, y (a nivel estatal) la División Oficina del Dato, puesta en marcha en julio de 2020.**
- **Como ejemplo regulatorio, el Decreto 76/2020 del 4 de agosto de 2020, aprobado en Cataluña, regula la gobernanza de la administración digital (arts. 5-9), así como el gobierno de los datos (Título II, arts. 10-26: modelo, protocolo, intercambio, interoperabilidad y acceso a datos, procesos y servicios digitales, gestión archivística de los datos y de los activos digitales).**

Hay que integrar las normas y los esquemas de estandarización y certificación que deban seguirse para lograr una ciudad segura, y hacer que estén alineados con las políticas regionales y nacionales. **Es preciso saber si en el país existe una estrategia nacional de ciberseguridad.**

**La Asamblea General de la OEA aprobó en 2004 la Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética (Barrero et al., 2018: 116). Muchos países de la región han adoptado estrategias nacionales de ciberseguridad, entre ellos: Argentina, Brasil, Chile, Colombia, Costa Rica, Guatemala, Jamaica, México, Panamá, Paraguay, República Dominicana, Trinidad y Tobago (BID y OEA, 2020: 180).**



Por lo general, y lamentablemente, estas estrategias no tienen en cuenta y no aplican directamente a las ciudades. No obstante, **la ciberseguridad urbana también forma parte de la ciberseguridad nacional**. La Alianza Global de Ciudades Inteligentes del G-20 (2021) señala su preocupación por la “mala conexión con políticas nacionales” de la ciberseguridad local. Soare y Burton (2020) hablan del “eslabón perdido” entre la ciudad inteligente y la seguridad nacional. ENISA (2015) recomienda que la “Comisión Europea y los Estados miembros aclaren las responsabilidades de cada agente en caso de incidente cibernético”, y la Directiva NIS (Directiva 2016/1148) de la Unión Europea se mueve en esta línea. La conexión entre la preparación para la seguridad subnacional y la responsabilidad nacional o federal fue objeto de análisis del informe de 2017 realizado por la Asociación Nacional de Gobernadores de Estados Unidos (García, Forscey y Blute, 2017). Por su parte, New America, Cohen y Nussbaum (2018) recomiendan una respuesta federal de financiamiento para conectar los programas regionales o locales con las prioridades nacionales y racionalizarlos. Asimismo, se recuerda que las relaciones entre las autoridades regionales y las ciudades están a veces tanto o más fracturadas que las nacionales o federales.

Esta situación se ha de remediar desde los niveles regionales y nacionales. No obstante, incluso supone una oportunidad para la ciudad. **Desde la ciudad se puede ser proactivo e intentar conectar la ciberseguridad urbana con la nacional**. Para ello, se deben identificar los canales o redes nacionales –o internacionales– sobre ciberseguridad. El lector o la lectora que tenga alguna responsabilidad en la materia, debe considerar que su ciudad puede pasar a ser pionera. Es posible participar o promover las redes de buenas prácticas de ciberseguridad entre las ciudades. Incluso se puede descubrir la existencia de programas de financiamiento para ciberseguridad.





**La ciudad debe conocer si cuenta con una legislación de ciberseguridad que deba seguir.** En cada país puede haber diferentes normativas en materia de ciberseguridad. Si esta normativa existe, las ciudades o quienes les prestan servicios y suministros (de telecomunicaciones o tecnológicos) deberían cumplirla. En la Unión Europea se ha buscado una homogeneidad y un estándar europeo común de ciberseguridad. Así, la Directiva NIS obliga a los Estados miembros a adoptar una estrategia nacional, e impone obligaciones para los prestadores esenciales y operadores críticos, esto es, aquellos cuyas rupturas de seguridad pueden generar importantes pérdidas financieras, menoscabar la confianza de la población, e incluso afectar la propia seguridad nacional. Estos sujetos obligados muchas veces operan y prestan servicios a las ciudades. A ellos se les insta a adoptar medidas para los niveles de riesgo, basadas en una evaluación previa de los mismos. Así, por ejemplo, estos prestadores y operadores están obligados a notificar incidentes de ciberseguridad, aunque no hayan tenido un efecto real, incluso con la finalidad de fomentar la cultura de gestión de riesgos. Hay una plataforma común de notificación que también podrá ser empleada para la notificación de vulneraciones de la seguridad de datos personales. El sistema es confidencial y se protege a la entidad notificante y al personal que informe sobre incidentes ocurridos, lo cual puede también involucrar a la ciudad. Las autoridades competentes ejercerán las funciones de vigilancia y promoverán el desarrollo de las obligaciones.

**En España, el sector público y las ciudades deben atenerse al Esquema Nacional de Seguridad (Real Decreto 3/2010, del 8 de enero de 2010) y las Guías de seguridad. Si la ciudad no cuenta con una legislación por seguir, este esquema y estas guías pueden ser un útil referente. Asimismo, la Directiva NIS se ha materializado principalmente a través del Real Decreto-Ley 12/2018, del 7 de septiembre de 2018, sobre seguridad de las redes y sistemas de información, mientras que el Real Decreto 43/2021, del 26 de enero de 2021, ha concretado obligaciones, medidas de seguridad y requisitos.**

Singapur lanzó su plan maestro nacional de ciberseguridad en 2013, al que siguió un nuevo proyecto de ley de ciberseguridad en 2016, que fue aprobado y se convirtió en ley en 2018. Ambas iniciativas forman parte de la Estrategia de Nación Inteligente de Singapur, uno de cuyos pilares es, precisamente, la ciberseguridad.<sup>11</sup>



George Kuenburg



Más allá de la legislación obligatoriamente aplicable, el equipo tecnológico debe conocer los variados estándares de ciberseguridad, privacidad y sus adaptaciones para IoT, telecomunicaciones y *smart cities*, y en lo posible debe optarse por seguir uno de ellos. En los últimos años se han ido desarrollando más estándares y normas comúnmente aceptadas, así como buenas prácticas. Cabe seguir los marcos estándar del sector para orientar las políticas de ciberseguridad de las organizaciones y la gestión de riesgos, como ENISA o NIST, así como ISO 2700, AICPA, CIS o COBIT. Asimismo, hay que tener especialmente en cuenta los estándares de ciberseguridad para IoT y telecomunicaciones provenientes de estas organizaciones, la Unión Europea o la OTAN. Más concretamente, respecto de la *smart city*, desde la Organización Internacional de Normalización (ISO) ya se contaba con la ISO 37120 sobre los indicadores para los servicios urbanos y la calidad de vida. En 2017 se adoptaron la ISO 37121, de desarrollo sostenible y resiliencia en las ciudades, y la ISO 37120, como plantilla para el desarrollo de las *smart cities*. En 2019 se adoptó la ISO 37122, con indicadores del progreso de ciudades inteligentes en economía, educación, energía, sostenibilidad, finanzas, gobernanza, salud, vivienda, población y condiciones sociales, recreo, seguridad, residuos, deporte y cultura, telecomunicaciones, transporte, agricultura urbana, y seguridad alimentaria y gasto en materia de agua. También se pueden utilizar estándares de seguridad específicos para el sector público y la ciudad. En el apartado técnico del capítulo 4 se facilitan los lineamientos básicos que una ciudad puede seguir a partir de estos sistemas.

11. Véase <https://www.smartnation.gov.sg/about-smart-nation/secure-smart-nation/cybersecurity-public-sector>.

Para el sector público nacional y local de Estonia, en el año 2000 se creó ISKE, un estándar de seguridad con implementación de estándares organizativos, de infraestructura y medidas técnicas de seguridad (Information System Authority, 2021).

En España, el Comité Técnico de Normalización 178 de AENOR sobre Ciudades Inteligentes y sus seis subcomités (infraestructura, indicadores y semántica, movilidad y plataformas de transporte, energía y medio ambiente, destinos turísticos, gobierno y servicios públicos 4.0) han publicado 31 normas de ciudad inteligente (UNE, 2021). Estas normas, que comenzaron a publicarse en 2012, facilitan la gestión y las estrategias de la ciudad inteligente, y permiten conocer el estado de conservación a lo largo de todo el ciclo de vida de los diferentes activos e infraestructura tecnológica de la ciudad, e incluso los riesgos y respuestas.

Por su parte, desde 2010, Estocolmo, Suecia, ha estado implementando directrices internas obligatorias de seguridad de la información que siguen ISO/IEC 27002. Además, se realizan numerosas actividades de sensibilización en ciberseguridad y se llevan adelante programas educativos, así como también se brinda apoyo para investigación y laboratorios de innovación para startups.

En 2014 la zona de Rennes St Malo, Francia, fue certificada con la etiqueta French Tech, “Capital tecnológica francesa” (La French Tech, 2019), ya que ocupa el primer lugar en telecomunicaciones, agroindustria y ciberseguridad, y lanzó el programa internacional Rennes Metropole de innovación, con fuertes alianzas empresariales y de investigación (Eurocities, 2016).



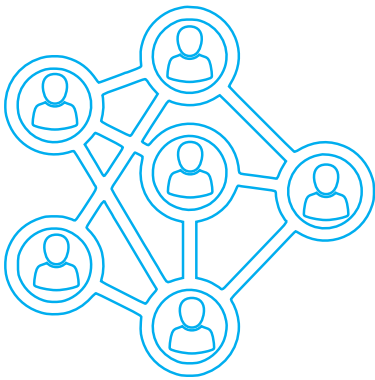


### 2.2.2

## Desarrollar políticas y normas de seguridad comunes con competencias claras y el compromiso de las partes

A partir de la legislación aplicable y de los estándares y modelos existentes, se debe proceder a dotar a la ciudad de una gobernanza que integre la de los datos, la *smart city* y la ciberseguridad.

En su medida 5, ENISA (2015) recomienda que los operadores, las ciudades y, en general, quienes busquen imprimir seguridad a sus procesos y servicios deben establecer las responsabilidades de la alta dirección en materia de ciberseguridad; esta definición de responsabilidades puede ser un incentivo para mejorar la ciberseguridad. Asimismo, New America, Cohen y Nussbaum (2018) insisten en la necesidad de codificar las funciones, responsabilidades y autoridades. Esta regulación debe ser una clara indicación del apoyo de los líderes con respecto a las iniciativas de ciberseguridad, y debe reducir posibles confusiones y conflictos. Se requiere un programa integral y centralizado de las múltiples partes implicadas, no solo las tecnológicas. Los conflictos entre diferentes órganos para integrar la ciberseguridad en los procesos son habituales; no obstante, la solución puede venir de la mano de superestructuras de ciberseguridad o de un coordinador o asesor en la materia.



**En esta línea, Japón (MIAC, 2020) recomienda:**

- I. Que sus ciudades desarrollen previamente normas de gestión de la seguridad, políticas de tratamiento de datos y criterios de riesgo que sean comunes para el conjunto.**
- II. Que sus ciudades definan las competencias de todas las partes; debe haber acuerdo previo sobre qué organización ha de captar los incidentes y cuál responderá. De lo contrario, se puede bloquear la prestación de servicios. Se recomienda establecer un diagrama de configuración y un diagrama del sistema y que se confirme que no hay áreas en blanco en la gestión.**
- III. Que todas las partes interesadas hayan conocido y deliberado I y II, esto es, las políticas, normas y competencias. Debe haber un foro dirigido por el promotor principal y, en la medida de lo posible, que todos hayan participado.**

También en NIST (2019) se señala la conveniencia de un consenso entre los líderes de la organización; en particular, sobre las prioridades de protección y privacidad, la tolerancia al riesgo y la asignación de recursos para implementar y supervisar los controles.

---

Desde el FEM, en junio de 2019, se creó la Alianza Global de Ciudades Inteligentes del G-20 sobre Gobernanza Tecnológica, que reúne a los gobiernos municipales, regionales y nacionales, a los socios del sector privado y a la sociedad civil, para recopilar y analizar políticas para ciudades inteligentes y éticas exitosas. Ya se cuenta con una hoja de ruta y una política de gobernanza (FEM, 2020; 2021). De ALC participan las ciudades de Bogotá, Brasilia, Buenos Aires, Córdoba (Arg.), Medellín, Ciudad de México y San José.

---

La mayoría de las 37 *smart cities* pioneras de la Alianza Global de Ciudades Inteligentes del G-20 cuenta con políticas de responsabilidad cibernética (28 de 37). Un tercio ha asignado un alto funcionario a la materia (13 de 28 ciudades), sus planes de gobernanza son revisados anualmente en 15 casos. Asimismo, la mitad mantiene un inventario actualizado (18 de 28). La función de TI no siempre está informada de los despliegues de nuevas tecnologías (11 de 28) (FEM, 2021).



## 2.3

# Institucionalizar la ciberseguridad

La institucionalización de la ciberseguridad se refiere a cómo integrar y ordenar entidades, recursos y el flujo de información con competencias claras y participación de las partes.

Uno de los cuatro elementos de la infraestructura de la *smart city* para el BID (Bouskela et al., 2016) es el Centro Integrado de Operación y Control (CIOC), habitual para ciudades de más de 200.000 habitantes. Los CIOC integran la estructura tecnológica (computadoras, sistemas de aplicaciones y monitores de los sistemas digitales), la infraestructura física (salas de operación, de gestión de crisis, etc.), la infraestructura de procesos, y el personal y los representantes de varios organismos públicos y proveedores de servicios, con un enfoque colaborativo y comprehensivo de los temas que serán tratados en lo que debe ser el cerebro de la ciudad inteligente. Estos centros se encargan de procesar y analizar los datos de la ciudad para la toma de decisiones inteligentes. En algunas ciudades, proceden de un ámbito sectorial que ha impulsado inicialmente la *smart city* –por ejemplo, movilidad, seguridad y respuesta a emergencias– y que luego ha ido integrando otros objetivos y funciones, como áreas de gestión de datos e inteligencia.



Sean o no un CIOC, toda ciudad debería tener un Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés). Se trata de un órgano principal supervisor que efectúa el seguimiento en tiempo real de la seguridad de la información y para ello analiza cualquier incidente que ocurra en la actividad de redes, servidores, aplicaciones, bases de datos, sitios web y otros sistemas. El SOC supone también un sistema de cooperación fluido donde se comparte la información con las múltiples partes interesadas, incluidos proveedores y operadores comerciales de los distintos servicios prestados. El SOC integra y comparte, si los hay, con los CSIRT o CERT, que son los equipos que preparan, coordinan y dan respuesta a incidentes de seguridad y emergencias informáticas. **Según las posibilidades de la ciudad, debe marcarse como objetivo la integración en un centro de tecnología, procesos, personal y representantes de los prestadores de servicios. Asimismo, esta integración debe permitir un seguimiento de los incidentes de seguridad en tiempo real y que se comparta información entre las partes.**



Como ejemplo mundial, especialmente de cara a su Expo 2020, a partir de 2013, Dubái pasó a ser referencia no solo en innovación tecnológica, sino también en infraestructura diseñada y seguridad estratégica. En 2014 se creó el Dubai Centre for E-Security,<sup>12</sup> el cual cuenta con una oficina de ciberseguridad en cada una de las 133 entidades y semi entidades gubernamentales. Además, anualmente, su marco de gobernanza de la ciberseguridad es revisado por la Oficina del Director General y evaluado por el Centro de Seguridad (Efthymiopoulos, 2016). Aunque se trata de una estructura nacional, este modelo puede inspirar proyectos regionales y de grandes ciudades.

.....

12. Véase <https://www.desc.gov.ae/about-us/#statement>.



### 2.3.1

## Designar a un responsable de ciberseguridad

El Oficial Principal de Seguridad de la Información (CISO, por sus siglas en inglés) es el director de seguridad de la información, papel ejecutivo para alinear la seguridad de la información con los objetivos de negocios y asegurar que la organización esté protegida. Por su parte, el Jefe de Información (CIO) es el director de las TIC y se encarga de que estas se alineen con las estrategias de la organización (INCIBE, 2016).

**Hay consenso internacional en concentrar en lo posible todas las responsabilidades de ciberseguridad de la ciudad en un “funcionario senior”,** que cabe interpretar como el CISO (FEM, 2020; Alianza Global de Ciudades Inteligentes del G-20, 2021). Sin embargo, se alerta de casos en que los CISO no tienen control efectivo y directo. Si un modelo concentrado no es posible, se propone un modelo de responsabilidad compartida entre un equipo central de tecnologías de la información (TI), en su caso el CIO, los departamentos de operaciones de la *smart city* y la oficina del CISO. En Japón se señala que la responsabilidad podría recaer en varios altos funcionarios, siempre y cuando no queden vacíos sin un responsable claro (MIAC, 2020). En estos supuestos debe haber una gran cooperación y coordinación entre los departamentos, CISO y CIO. New America, Cohen y Nussbaum (2018) advierten de los impedimentos que existen para concentrar la ciberseguridad en una figura o institución, especialmente debido a sistemas y organizaciones heredados y a las dificultades inherentes a integrar departamentos y servicios. En todo caso, insisten en la conveniencia de una estructura de ciberseguridad o un coordinador o asesor de ciberseguridad empoderado que se sitúe por encima de los organismos existentes para establecer prioridades y coordinar o dirigir esfuerzos.

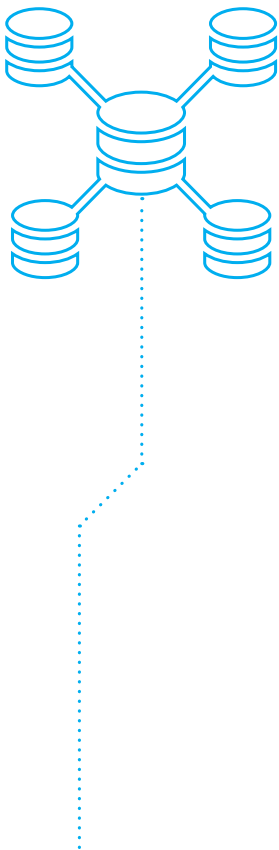
Debe valorarse la conformación de un equipo mínimo de ciberseguridad, liderado por el CISO, un oficial de protección de datos personales, un experto en pruebas de penetración y el equipo de apoyo, según las actividades identificadas para las capacidades de ciberseguridad. El CISO se debe articular con el CIO de la organización. Para ello, se puede recurrir a la figura de comité de ciberseguridad. Dicho comité puede tener una versión local para la entidad y otra a nivel del sector. Para cada rol se deben definir competencias genéricas (blandas) y habilidades de ciberseguridad (duras), y establecer perfiles.

En algunas ciudades no hay un CISO o un CIO; como máximo, puede haber un responsable de tecnología. Entonces, en lo posible, deben concentrarse y aclararse sus responsabilidades. Aunque lo deseable es contar con personal interno de la ciudad, en ocasiones los servicios especializados de un CISO pueden externalizarse, como sucede con los delegados u oficiales de protección de datos en muchas ciudades (AEPD, 2018).



### 2.3.2

## Determinar las funciones del responsable de ciberseguridad



Este funcionario senior o CISO **es el responsable de que se cumplan todas las medidas de ciberseguridad, específicamente las dirigidas al personal técnico** y se observen los estándares y regulaciones aplicables. Es quien lidera la rendición de cuentas con autoridad para ejecutar la ciberseguridad para toda la infraestructura de TI y tecnología operativa (usuarios, dispositivos, redes, datos y aplicaciones). Debe tener conexión directa con la autoridad máxima de la ciudad. Ha de ser miembro del equipo de liderazgo de alto rango del ayuntamiento o depender directamente del mismo. El CISO asume como funciones principales las “responsabilidades críticas” (Alianza Global de Ciudades Inteligentes del G-20, 2021: 7 y ss.), que pueden verse en el apartado 4.3 de esta guía.

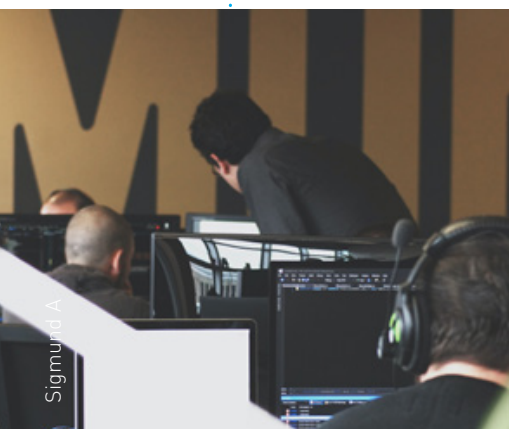
Adicionalmente, pero también bajo su égida, habrá responsables específicos para la seguridad de redes y de aplicaciones, el monitoreo de activos, el registro de la capacitación en seguridad de la información y gestión de riesgos, lo que deberá realizarse con una frecuencia al menos anual; la realización de auditorías o designaciones de terceros; el establecimiento de una política de evaluación de riesgos y de investigación para terceros con los que se subcontraten actividades; y responsables de que haya materiales educativos para la ciudadanía sobre temas básicos de ciberseguridad (Alianza Global de Ciudades Inteligentes del G-20, 2021: 10 y ss.).

### 2.3.3

## Establecer mecanismos para compartir información de ciberamenazas con los diversos actores

**Los actores públicos y privados deben compartir, con confianza y confidencialidad, información de ciberseguridad y de los incidentes acaecidos, sobre la base de estructuras y puntos de contacto y cooperación establecidos.**

ENISA (2015) señala que es imprescindible el intercambio transversal y proactivo de información sobre amenazas e incidentes para conocer y poder dar respuestas armonizadas. También se torna indispensable la confianza entre las partes para evitar costes de reputación.







Para ello, pueden resultar útiles los modelos de anonimización de confidencialidad. Sin embargo, por lo general, en las ciudades inteligentes falta una arquitectura de referencia para el intercambio de datos. En función de ello, NIST (2019) indica que se precisan consensos, y la modificación de las estructuras y procesos existentes, así como de los servicios compartidos. Todas las partes interesadas deben establecer un punto de contacto en caso de que se produzca una situación de emergencia. En el caso de prestadores y proveedores, los contratos han de aclarar y detallar la información que se manejará, y resaltar la responsabilidad y la comunicación entre las partes.

La ciudad debe imponer o tener previstos canales de comunicación con respecto a incidentes de ciberseguridad entre las diferentes áreas o servicios de la propia ciudad, así como con todos los proveedores y prestadores externos.

#### **Dentro de sus responsabilidades, los líderes y gerentes urbanos deberían:**

- **Definir** un punto de contacto con respecto a los incidentes.
- **Dar** a conocer la existencia de confidencialidad para los niveles técnicos y tecnológicos, y para los prestadores de servicios si remiten información.
- **Imponer** obligaciones de repore de incidentes en los contratos de los proveedores.
- **Realizar** prácticas con equipos pequeños que integren diferentes áreas o servicios urbanos, así como prestadores u operadores, lo cual genera dinámicas o confianza para compartir información.
- **Tener** también prevista la comunicación con responsables de niveles superiores regionales o del ámbito nacional.

**No hay un solo modelo para seguir. El sector público y el privado han creado sistemas de intercambio de información de ciberseguridad. New America, Cohen y Nussbaum (2018) ofrecen las mejores prácticas de gobernanza de la ciberseguridad de la *smart city*, y destacan en particular el caso de Arizona (interfaz ACTRA), Nueva Jersey (superestructura burocrática NJCCIC, lugar común que es punto de contacto y coordinación), así como el modelo de la Oficina de Ciberseguridad integrada en la Agencia Washington Technology Solutions (WaTech), que comprende competencias de gestión militar y de emergencias.**

## 2.4

# Integrar la seguridad de los datos confidenciales de la ciudad y los datos personales

### 2.4.1

## Manejo de datos

Cada vez más, la ciudad obtiene una utilidad de los datos masivos, mediante su captación, recopilación, almacenamiento, análisis y extracción de valor para la toma de decisiones y prestación de servicios. Toda la información y los datos de la ciudad deben ser protegidos, si bien esto debe hacerse según su criticidad y nivel de riesgo. Para ello, **se deben identificar y valorar los datos críticos, así como los especialmente confidenciales para la urbe**. A tal fin, hay que conocer la normativa aplicable, así como valorar los datos según se relacionen con activos, estrategias, intereses, funciones y operaciones de la ciudad. También se debe ponderar si una ruptura en la seguridad de estos datos puede generar un perjuicio directo al ciudadano, pérdidas económicas, daño reputacional o protestas. Para esta identificación y evaluación los niveles técnicos y administrativos **cuentan con diversos recursos** del NIST (2008), el CCN (2020) o la OEA (2019). A partir de allí, a los datos habrá que aplicarles la ciberseguridad correspondiente a su valor y nivel de riesgo.

Cabe detenerse ahora especialmente en los datos personales y los especialmente protegidos. Muchos de los datos que maneja la ciudad, en principio, no son personales, pues no se pueden vincular a personas concretas. Sin embargo, **cada vez más se generan masivamente datos que sí son personales**. Así sucede por la tendencia a la personalización de servicios y visiones 360° o, también, por la sensorización de personas y el creciente empleo de *apps* de la ciudad vinculadas a sus terminales móviles. Especial sensibilidad tienen los datos de geolocalización, tan habituales en la ciudad inteligente. Y mayor protección debe darse si se vinculan a reuniones o manifestaciones políticas o sindicales, centros médicos o religiosos, pautas de comportamiento ligadas a la vida sexual, etc. (AEPD, 2020b; Grupo del Artículo 29, 2011).

**Si los datos que maneja la ciudad son vinculables a ciudadanos concretos, se trata de datos personales y entonces pasa a aplicarse la amplia y rigurosa normativa de protección de datos**. Mayores serán aún las garantías y las exigencias de seguridad si, además, los datos son especialmente protegidos (de corte racial, ideológico, sindical, sanitario, genético, sexual o de identificación biométrica) o refieren a delitos y sanciones.



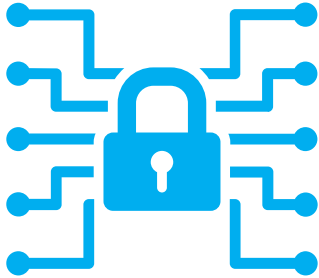


Con los datos personales debe seguirse el principio de responsabilidad proactiva: la ciudad que trate datos personales ha de cumplir toda una serie de obligaciones y tiene que poder probar que las ha cumplido. Asimismo, los procesos y procedimientos de la ciudad que manipulen datos deben seguir las normas de privacidad en el diseño y por defecto. Bajo el principio de minimización, desde el minuto cero, la ciudad deberá usar la mínima cantidad de datos que sea posible y durante el mínimo tiempo posible. Ello se contrapone a la extracción y explotación masiva de datos, que es la esencia misma de la ciudad inteligente. La minimización impone limitar la georreferenciación de *smartphones*, sensores de la ciudad o *apps* de la ciudad o sus proveedores. Además, resulta imprescindible hacer depuraciones de información periódicamente para evitar la acumulación de datos que no se correspondan con las finalidades legítimas o sean desproporcionados. Es preciso determinar plazos de conservación de datos según sus finalidades, su sensibilidad y sus riesgos (AEPD, 2017: 12, 17). Pasado el plazo, los datos deben dejar de ser utilizados por la ciudad, en lo posible deben mantenerse encriptados y ser solo accesibles de manera restringida. Siempre que la legislación aplicable (sobre archivos, transparencia, responsabilidades administrativas o sancionatorias, etc.) lo permita, los datos han de ser finalmente destruidos. Si resulta posible, las copias de datos deben ser automatizadas.

**Santander es una de las ciudades inteligentes de referencia en España (por ejemplo, en gestión del alumbrado público y recolección de residuos). También se destaca por aplicar la privacidad y seguridad desde el diseño. Los responsables de ciberseguridad y las empresas participan en la definición de las acciones de ciudad inteligente antes de su implantación, y determinan las medidas por aplicar. Así, por ejemplo, en razón de la COVID-19, se ha establecido un sistema completo de control de la afluencia de personas en dependencias municipales.**

De acuerdo con el principio de lealtad, la ciudad solo podrá manejar los datos para las finalidades habilitadas desde el punto de vista jurídico y legítimo. Por lo general, pueden manejarse datos para la administración, la gestión de impuestos, la prestación de servicios sociales, educativos o de salud, etc. Lo que no está tan claro es que la ciudad inteligente pueda reutilizar esos datos para prestar mejor esos u otros servicios, para evaluar, monitorear, controlar o decidir políticas públicas, etc. Muchas veces las leyes no son suficientemente claras ni respecto del uso de datos personales por parte de las ciudades ni, en concreto, para los proyectos de ciudad inteligente.





Como excepción positiva, cabe mencionar el UK Digital Economy Act de 2017, sec. 35.<sup>13</sup> **Debe vigilarse que el proyecto o tratamiento de datos personales cuente con suficiente cobertura legal.**

En todo tratamiento masivo de datos que realice la ciudad, y antes del despliegue de un proyecto de ciudad inteligente, **es obligatorio hacer un análisis de riesgos y muy posiblemente un estudio completo de impacto de protección de datos** (art. 35 del Reglamento General de Protección de Datos [RGPD];<sup>14</sup> AEPD, 2018; AEPD, 2020a: 22). Así, debe valorarse la información y el volumen de datos que se hayan de manejar, las fuentes y la conservación, y deben determinarse los riesgos e impactos, y conforme a ellos, las medidas de seguridad y organizativas que se deban implantar. La AEPD (2021) explica cómo hacerlo en su [Guía de Evaluaciones de Impacto](#). **En virtud de la íntima conexión y las similitudes existentes en la materia, el cumplimiento de la protección de datos debe vincularse a las acciones de ciberseguridad.**

**La explotación de los datos por parte de la ciudad se ha vuelto cada vez más intensiva y ha ido incorporando masivamente capas de inteligencia artificial. Por eso, deben tenerse en cuentas las cautelas y auditorías obligatorias.** En esencia, debe hacerse una gestión de la calidad de los datos de entrada y de los utilizados para el entrenamiento del sistema, además de un control de sesgos y de las garantías de robustez del sistema de inteligencia artificial; verificar que se generen los registros o logs que permiten comprobar el funcionamiento y los eventos ocurridos, y realizar un monitoreo de la trazabilidad, la transparencia, la explicabilidad y la recurrencia, así como una auditoría constante y una evaluación. Para ello, pueden seguirse las guías de inteligencia artificial de la AEPD ([2020a](#) y [2021](#)).

**Cabe destacar la creación, en 2020, del Registro de algoritmos<sup>15</sup> de la ciudad de Ámsterdam, el cual permite una gran transparencia ciudadana en cuanto al uso de inteligencia artificial en la ciudad inteligente. Este presenta descripciones generales y también técnicas y la posibilidad de participar de iniciativas.**

**Asimismo, el 30 de junio de 2021 Barcelona, Londres y Ámsterdam crearon el Observatorio Global de Inteligencia Artificial para controlar la aplicación ética de la inteligencia artificial en las ciudades. En la iniciativa colaboran UN-Hábitat y el CIDOB-Centro de Asuntos Internacionales de Barcelona.**

13. Véase <https://www.legislation.gov.uk/ukpga/2017/30/section/35>.

14. Véase <https://www.boe.es/doue/2016/119/L00001-00088.pdf>.

15. Véase <https://algorithregister.amsterdam.nl/en/ai-register/?s=08>.



**«La esencia de la ciberseguridad abarca el conocimiento y la comprensión del entorno, la planificación, la proactividad en materia de prevención y la constante vigilancia, la colaboración y cooperación, el entrenamiento y la capacitación permanentes.»**



## 2.4.2

# Anonimización y seudonimización, estrategia y medida de seguridad esencial para que la ciudad maneje datos

Según ya se ha puntualizado, es menester identificar, evaluar y aplicar a los datos e información las medidas de seguridad correspondientes al nivel de riesgo. En todo caso, cabe señalar que **muchas dificultades para cumplir con la normativa de protección de datos pueden resolverse si se logra que los datos se desvinculen de las personas concretas que los generan**. Se trata de una preocupación para los gestores de las ciudades que el BID ya ha identificado (Cerdeira et al., 2020: 28). Para ello, se deben anonimizar los datos de acuerdo con los estándares establecidos por las autoridades de protección de datos (AEPD, 2019a; ICO, s.f.). Si los datos se anonimizan por completo no habrá necesidad de aplicar la normativa de datos y la ciudad y sus proveedores podrán utilizarlos con libertad y menos medidas de seguridad. Ahora bien, la anonimización total es cada vez más difícil de lograr, pues cada vez hay mejores tecnologías para revertir la anonimización y reidentificar a las personas.

Una estrategia esencial es la seudonimización. **Se trata de anonimizar en lo posible los datos** y que los diferentes servicios de la ciudad o los prestadores y empresas los manejen así para explotar y extraer su valor sin que sean datos personales. Al mismo tiempo, los datos no personales permanecen aislados de los departamentos u órganos de la ciudad que sí tienen la capacidad de reidentificación. Así, de producirse rupturas o fugas, solo se accederá a datos no personales. Además, **si hay seudonimización, legalmente es mucho más fácil que la ciudad pueda explotar datos de sus ciudadanos para finalidades relacionadas con la ciudad inteligente, estadísticas, investigación, etc.**





## 2.5

# Integrar los proveedores a la ciberseguridad

**La ciberseguridad debe integrarse en la elección, contratación y gestión de proveedores y prestadores de servicios.** Para ello, pueden seguirse algunos lineamientos de contratación como los fijados recientemente para la contratación en salud ([ENISA](#), 2020).

De acuerdo con NIST (2019), **ello permite que la ciudad mantenga el control y dicte los requisitos de gestión de riesgos y evita que sean los proveedores quienes se los impongan a la ciudad.** Sin embargo, Ranchordás y Goanta (2020) alertan que las ciudades acaban plegándose a las condiciones marcadas por las grandes plataformas, en perjuicio de los valores e intereses comunes, la ciberseguridad y los derechos de la ciudadanía. Frente a ello es del todo aconsejable que las ciudades compartan información sobre los proveedores y prestadores y establezcan cláusulas y contratos tipo. Soare y Burton (2020) consideran “paradójico” que la contratación pública todavía no se centre lo suficiente en la ciberseguridad. El CISO-funcionario senior tiene entre sus responsabilidades esenciales adoptar las decisiones de ciberseguridad de cualquier inversión significativa en productos o servicios de TI y tecnología operativa adquiridos por la ciudad. Shacklett (2019) insiste en que la normativa relativa a la seguridad de las TI debe cumplirse a rajatabla. Los fabricantes y proveedores deben seguir enfoques de seguridad desde el diseño de las tecnologías y servicios adquiridos, como los fijados en general por ENISA (2014): seguridad por diseño, menor privilegio (restricción de permisos), autenticación fuerte, protección de activos, seguridad de la cadena de suministro, transparencia de la documentación, gestión de la calidad, continuidad del servicio y restricción del uso de datos.

En los pliegos y la contratación, conviene seguir estos lineamientos:

- Garantizar requisitos de ciberseguridad en el nivel de prestación de servicios (SLA, por sus siglas en inglés) (FEM, 2021). Asimismo, hay que evitar la fuga de información en el subcontratista (MIAC, 2020).
- Establecer un plan específico de respuesta a incidentes (Cerrudo, Asbini y Russell, 2015). También ha de incluirse el soporte para incidentes 24/7/365.



- Establecer las pruebas a las que se someterá el sistema y determinar la exigencia de certificaciones de terceros. También se han de permitir la auditoría y los registros, y debe acordarse la entrega de informes de auditoría de seguridad con periodicidad anual.
- Definir quién y de qué manera se ejercen la vigilancia y el control del cumplimiento de las obligaciones de ciberseguridad que deben acatar los terceros y subcontratados.
- Definir qué información se va a compartir, cuáles serán las funciones y responsabilidades, etc. (MIAC, 2020). Debe detallarse un sistema efectivo de notificación y corrección de vulnerabilidades que involucre a los proveedores (ENISA, 2015). Para ello, ha de garantizarse la interoperabilidad.
- Convenir acuerdos de confidencialidad que permitan compartir información de incidentes sin necesidad de su difusión (NIST, 2019).

Forrest (2019) añade **algunos elementos para tener en cuenta al elegir proveedor**; por ejemplo, si puede generar una publicidad negativa o desconfianza en los contratantes. Desde el punto de vista financiero, cabe tener en cuenta si es rentable, si tiene otros grandes clientes, cuál es su estrategia de salida. Puede ser de interés acudir a empresas especializadas en determinar el perfil de los proveedores y sus riesgos. Sin perjuicio de todas las prevenciones por adoptar, en el caso de proveedores emergentes en proyectos de innovación y piloto puede ser interesante flexibilizar las exigencias.

**La normativa de protección de datos suele obligar a determinados contenidos en los contratos y diversos aspectos están directamente relacionados con medidas de seguridad.** Así, los contratos de la ciudad con la empresa deben regular las relaciones entre el responsable (la ciudad) y el encargado del tratamiento (contratista) y detallar las instrucciones para este último, el deber de confidencialidad, las medidas de seguridad aplicables, las posibilidades de subcontratación, los derechos de los interesados, las obligaciones de colaboración, el destino o la eliminación de los datos tras el servicio, así como los medios con que cuenta la ciudad para controlar que se cumplan dichas condiciones. Para ello, se pueden seguir el modelo y las Directrices de contratación de la AEPD (2019b). Si las empresas utilizan los datos para otras finalidades de su propio interés, eso debe quedar claro en el contrato y pasarán a ser responsables o corresponsables en términos de protección de datos.



## 2.6

# Formar, comunicar y concientizar acerca de la ciberseguridad

La ciberseguridad requiere formación, comunicación y concientización. Por ello, el responsable de alto nivel o gerente de la ciudad debe establecer los planes de formación, y los planes de concientización y comunicación.

### 2.6.1

## Establecer los planes de formación

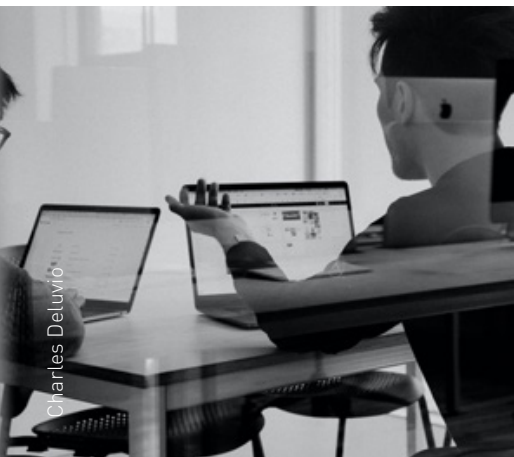
De acuerdo con Stuart Chontos- Gilchrist, de E3 Technology, muchas veces “las empresas están reconociendo que son las personas, más a menudo que las máquinas, las que generan las brechas de seguridad”.<sup>16</sup> Los atacantes siempre buscan el eslabón más débil y por lo general los vectores de ataque incluyen no solo la tecnología, sino también a los empleados (ENISA, 2015, apartado 5.1). El factor humano lo es todo y las amenazas humanas son las más relevantes (NCSC, 2021). Los directivos y el personal han de estar sensibilizados, formados y actualizados para actuar correctamente (Bouskela et al., 2016: 45; Shacklett, 2019).

El alto funcionario responsable de ciberseguridad lo es también de **la formación periódica de los empleados, que debe estar bien planificada y dotada de recursos**. Como puntualiza Stilgherrian (2019), la formación en seguridad no sirve de nada si no cambia los comportamientos y si no hay un compromiso. Hay que buscar el compromiso y el cambio cultural. Para ello, es esencial, en primer lugar, formar al personal en materia de seguridad electrónica personal (redes, familia, hogar, menores, acoso, etc.). Así, luego será mucho más fácil involucrarles en los problemas de ciberseguridad de la organización y en las buenas prácticas, como, por ejemplo, no repetir ni compartir contraseñas, actualizarlas con frecuencia, no responder mensajes sospechosos, no enviar información por canales no seguros, no utilizar los equipos públicos para finalidades privadas (y a la inversa), no instalar programas no autorizados en sus dispositivos, etc. Tómese en cuenta la utilidad de incentivar el compartir experiencias y temores de seguridad con los colegas (véase la experiencia “*It’s time to #askoutloud about cyber safety, Stay Smart Online*” del gobierno australiano).<sup>17</sup>

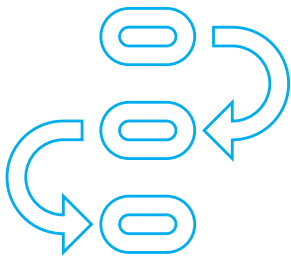
.....

16. Véase <https://www.e3security.com/about>.

17. Véase <https://www.acic.gov.au/media-centre/media-releases-and-statements/its-time-askoutloud-about-cyber-safety>.



Charles Deluvio



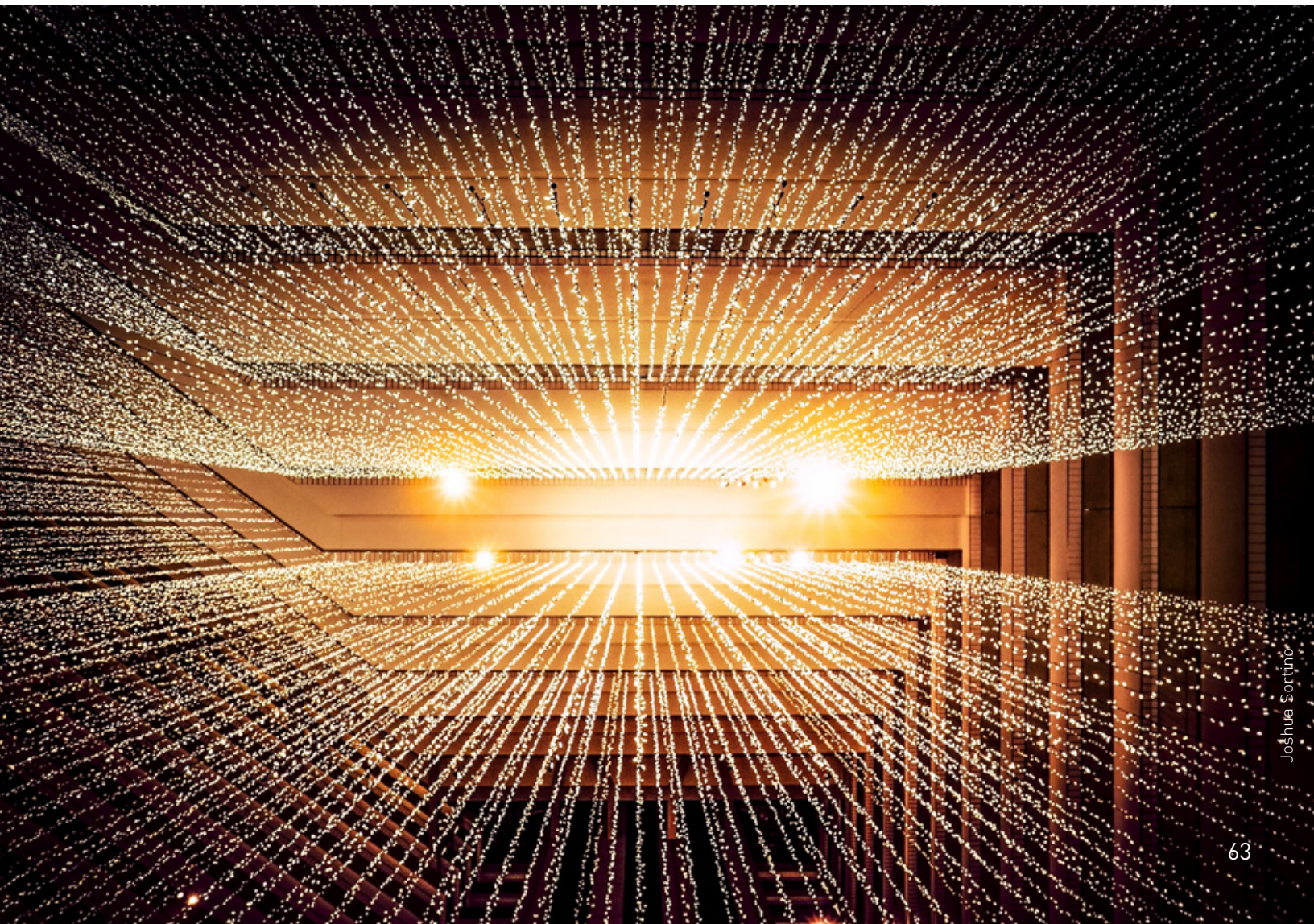


### 2.6.2

## Establecer los planes de comunicación

**Los responsables de la seguridad han de explicar claramente las tecnologías, políticas y prácticas de ciberseguridad en un lenguaje sencillo que puedan entender el alcalde, los directivos y los ejecutivos de la ciudad ajenos al campo tecnológico.** La dirección debe comprender por qué está promulgando regulaciones o políticas, o haciendo una importante inversión. Si no lo entiende, no podrá exponerlo ni defenderlo. Y todo ello, obviamente, sin necesidad de que se presente un problema de seguridad que lo haga todo evidente.

Igual de importante es la comunicación aguas abajo. **Las políticas y la normativa de ciberseguridad son áridas, complejas y nada motivadoras para los empleados.** Hay que invertir en una buena comunicación de las mismas y, como se ha mencionado, lograr que el personal se apropie de las preocupaciones.





## 2.7

# Disponer de financiamiento y seguros para la ciberseguridad

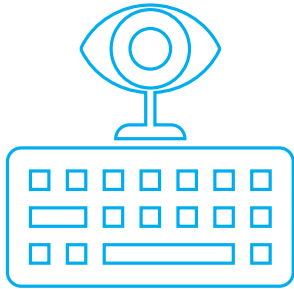
**Una *smart city* requiere seguridad financiera** (Townsend y Zambrano-Barragán, 2019: 39) **y la ciberseguridad precisa presupuesto, el cual, si no se destina a tiempo, aumenta cada vez más. El coste social, político, económico y de confianza por no invertir a tiempo puede ser enorme.** ENISA (2015) señala que el conocimiento y el gasto en ciberseguridad son relativamente muy bajos en comparación con los impactos de potenciales ataques (como los referidos en el apartado 1.4.3); por eso, su Recomendación N.º 7 es que los operadores y prestadores y los ayuntamientos inviertan un mayor presupuesto en ciberseguridad, en particular para sensibilizar y brindar formación a todo el personal y los altos directivos, además de llevarlos a desarrollar conocimientos, etc., así como para facilitar la recepción de soluciones provenientes de terceros que cumplan con los requisitos de seguridad.



Hay que planificar los recursos y también deben computarse las revisiones del diseño del sistema, las pruebas, la supervisión activa del tráfico de la red, los seguros, y los costes técnicos, contractuales y legales asociados a la reparación y recuperación de una brecha. Los sistemas obsoletos y desactualizados ponen en jaque la ciberseguridad. Soare y Burton (2020) señalan que los períodos prolongados de austeridad presupuestaria establecidos desde 2010 fueron negativos y la recesión económica derivada de la crisis de la COVID-19 puede empeorar la situación.

En las fases iniciales la ciudad también debe valorar **la contratación de un seguro de ciberseguridad** y, por supuesto, integrarlo en sus presupuestos. Según una encuesta del *Wall Street Journal*, la mayoría de las 25 ciudades más grandes de Estados Unidos cuentan con un seguro cibernético o están considerando adquirirlo (NIST, 2019). Los seguros pueden dar cobertura a los daños (incluso los reputacionales) que se produzcan por un ataque. Pueden incluir servicios para minorar daños, recuperar datos y equipos, proteger identidades y responder a las reclamaciones de terceros. Asimismo, **si la ciudad cuenta con un seguro se pueden generar positivas dinámicas preventivas.** Normalmente, los seguros incluyen algunos servicios de prevención y asesoramiento para el cumplimiento normativo.





Además, imponen obligaciones preventivas de ciberseguridad. En consecuencia, la contratación de un seguro, además de limitar los daños en caso de ataques, estimula la realización periódica de evaluaciones, el dictado de cursos de formación, la actualización de equipos, la preparación de copias de seguridad y otras medidas.

Hasta aquí, se han expuesto recursos, recomendaciones y las mejores prácticas para responder a las ciberamenazas desde la ciudad. Lo primero es tomar en cuenta la complejidad del ecosistema y sus numerosos actores. Se han señalado las claves de políticas, normas, órganos, responsabilidades y fórmulas de gobernanza adecuadas, con una buena conexión con los niveles regionales y nacionales de ciberseguridad. La ciudad maneja muchos datos personales y confidenciales, y tiene que analizar los riesgos e implantar medidas de seguridad acordes a los mismos. Se ha aconsejado especialmente la anonimización y seudonimización de los datos como una estrategia legal y de seguridad básica. Se ha insistido en la importancia de compartir información entre las partes, y también se han subrayado las claves necesarias para la contratación y selección de prestadores y proveedores. En cualquier caso, la concienciación y formación de responsables y personal de la ciudad sigue siendo una de las mayores inversiones que se debe realizar. Todo ello, precisa recursos y presupuestos. Esta hoja de ruta, que se resume en el gráfico 2.2, sirve para todo tipo de ciudades: no hay que esperar a mañana para llevarla a la práctica.





# Hoja de ruta de las responsabilidades en materia de ciberseguridad urbana



## Líderes de gobierno

1. Definir la visión y los objetivos de la iniciativa de ciberseguridad; para ello, establecer el sector o los sectores dentro del alcance.
2. Establecer las normas y políticas necesarias: acuerdos, ordenanzas, decretos, resoluciones o actos administrativos, alineados con la estrategia regional y nacional de ciberseguridad; incorporar los estándares dentro de las normas.
3. Crear la institucionalidad que materialice la ciberseguridad; determinar los responsables y sus funciones; establecer un esquema de coordinación para hacer frente a incidentes.
4. Disponer las líneas para que se identifiquen y valoren los datos críticos, así como los especialmente confidenciales para la ciudad.
5. Establecer una directiva municipal para que se integre la ciberseguridad en el proceso de selección, gestión y contratación de prestadores de servicios.
6. Establecer una directiva municipal para adelantar los procesos de formación y comunicación.
7. Establecer una directiva municipal para adelantar los procesos de financiamiento y adquisición de seguros.



## Gerentes municipales

1. Identificar los servicios que se van a proteger; definir los planes, programas y proyectos alineados con las políticas, de la mano del equipo técnico; identificar los actores involucrados.
2. Generar los procesos para el cumplimiento y la materialización de las normas y políticas.
3. Establecer los procesos y procedimientos internos para materializar la institucionalidad en el sector.
4. Establecer los procesos y procedimientos internos para identificar y valorar los datos críticos, así como los especialmente confidenciales para la ciudad.
5. Integrar la ciberseguridad en el proceso de selección, gestión y contratación de prestadores de servicios.
6. Instaurar un plan de formación y comunicación en el sector.
7. Establecer un plan de financiamiento del sector y adquisición de seguros.



## Personal de tecnologías de la información

1. Identificar información asociada a los servicios y los activos de apoyo que se van a proteger.
2. Cumplir y ejecutar las normas y políticas dispuestas para la función de ciberseguridad; identificar el modelo de ciberseguridad por implementar.
3. En el marco del modelo de ciberseguridad, definir las capacidades por implantar; para ello, habrá que integrar los procesos, la tecnología y la información en la institucionalidad.
4. Identificar y valorar los datos críticos, así como los especialmente confidenciales para la ciudad.
5. Establecer los requisitos básicos de seguridad que se deben incorporar en el proceso de adquisición de productos y servicios de tecnologías seguros.
6. Ejecutar el plan de formación y comunicación de la iniciativa.
7. Ejecutar el plan de financiamiento de acuerdo con la hoja de ruta trazada y los recursos asignados.

Fuente: Elaboración propia (2021).

Nota: Las responsabilidades presentadas en este gráfico se deben articular con las responsabilidades que se establezcan en el personal de nivel intermedio entre los líderes municipales y los gerentes municipales, y, a su vez, entre estos y el personal de ciberseguridad y TI.

# 3

## ***Decálogos de ciberseguridad para personal de los niveles estratégico, táctico y operativo o técnico***



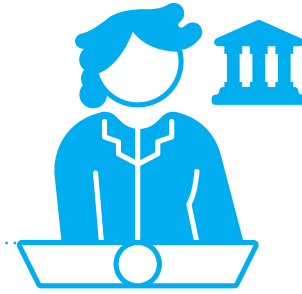
***«La ciberseguridad está en manos de los administrativos, secretarios, así como de los empleados de la ciudad que realizan acciones específicas para ejecutar políticas, planes y programas y profundizan también en cada área específica de la ciudad.»***



### 3.1

## Decálogo para alcaldes y líderes de alto nivel

### Líderes de gobierno - Nivel estratégico



La ciberseguridad depende de la dirección general ejecutiva, así como de la visión, el liderazgo, la acción estratégica y la fijación de objetivos con determinación de políticas y gestión de recursos. En función de ello, cabe resaltar las siguientes recomendaciones:

1. **Generar acuerdos políticos** con los distintos sectores. La ciberseguridad es una política de toda la ciudad y excede un mandato electoral; requiere consensos, recursos y visión a mediano y largo plazo. Ello facilitará la priorización y asignación de los recursos requeridos en la materia.
2. **Enviar mensajes políticos destinados a sensibilizar** a los funcionarios y también a la ciudadanía para lograr apoyo político. No hay que esperar a sufrir un ataque cibernético para comprender los impactos que provoca.
3. **Aunar en una sola voz toda la política de ciberseguridad.** Hacer que las partes involucradas adopten estrategias, políticas, normas y competencias claras en materia de ciberseguridad. Con su liderazgo, el alcalde o la persona responsable otorgan legitimidad y refuerzan las acciones para unir los divergentes ámbitos que abarcan los sectores público y privado.
4. **Establecer institucionalidad** y valorar la creación de un área de coordinación y centros de control con atribuciones bien definidas en el ámbito de la ciberseguridad. Dotarlos de recursos y apoyar especialmente su integración y cooperación.
5. **Estimular la concienciación**, formación y capacitación permanente en ciberseguridad de los directivos y el personal, y lograr que haya campañas para la ciudadanía. La ciberseguridad depende de todas las personas. Vigilar que normas, políticas y planes no se queden en los “cajones” y fomentar las pruebas, los simulacros y la evaluación continua.
6. **Involucrar al sector privado** que presta servicios y suministros a la ciudad. Mantener esquemas de coordinación y confianza. Vigilar que el ayuntamiento lidere los términos de contratación y que en estos se incorpore la ciberseguridad, incluso en las *startups* y pequeñas y medianas empresas (pymes), a través de políticas, planes y financiamiento.
7. **Estimular la actualización y renovación de activos tecnológicos** obsoletos y la adquisición de bienes y servicios con seguridad en el diseño, que automaticen la ciberseguridad y empleen tecnologías emergentes.
8. **Asegurarse de que la ciberseguridad forme parte de los elementos por evaluar** en las políticas de la ciudad y en especial de la ciudad inteligente.
9. **Emplear mecanismos de planificación financiera** que permitan mantener los proyectos a corto, mediano y largo plazo. Recordar que la ciberseguridad necesita recursos y financiamiento.
10. **Fomentar la participación de la ciudad en redes de ciberseguridad** nacionales para las ciudades. Los programas locales de ciberseguridad se deben alinear con las estrategias metropolitana y nacional. Prestar especial atención a los recursos que se ofrecen en el nivel nacional o federal, e incluso internacional.

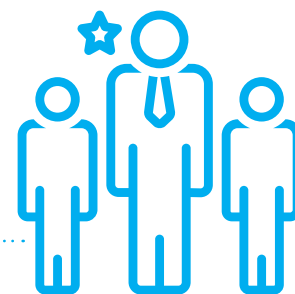




## 3.2

# Decálogo para secretarios municipales y empleados

## *Gerentes municipales - Nivel táctico*



Sin perjuicio de las decisiones estratégicas, la ciberseguridad está en manos de los administrativos, secretarios y empleados de la ciudad que realizan acciones específicas para ejecutar políticas, planes y programas, y profundizan también en cada área específica de la ciudad. Valgan las siguientes recomendaciones para ellos, según su posición y responsabilidades:

1. **La ciberseguridad empieza en cada uno**, en su computadora y su terminal móvil. Identificar bien la tecnología y la infraestructura que se debe proteger desde el punto de vista cibernético, así como los actores involucrados.
2. **Conocer y comprender las amenazas** a las que se está expuesto en el ciberespacio. En la medida de lo posible, realizar una autoevaluación o un diagnóstico del nivel de madurez en ciberseguridad.
3. **Conocer qué acciones concretas, estrategias, normas**, políticas y procedimientos de ciberseguridad tiene su ciudad y cuáles son sus responsabilidades. Si es de su competencia, que sus subordinados las conozcan también.
4. **No dejar las políticas y normas en el cajón**. Poner a prueba las propias responsabilidades, participar de simulacros, y adoptar los procesos y procedimientos. Si se detecta una falla de seguridad en el ayuntamiento o en la empresa que presta servicios, esto se debe comunicar al órgano competente, incluso de manera confidencial.
5. **Participar en los programas de formación** y actualización para llevar a cabo las responsabilidades de ciberseguridad.
6. **Comunicar bien las políticas y directrices** para que todos se apropien de ellas. Compartir las propias experiencias de ciberseguridad con sus compañeros, con otras áreas, así como con otros gobiernos locales.
7. **Preguntarse si se cuenta con los recursos materiales**, humanos, financieros y técnicos necesarios para las responsabilidades de ciberseguridad. Si son insuficientes, planificar y solicitar la dotación de recursos necesaria.
8. **Si corresponde, planificar y estructurar los recursos humanos**, integrando personal adecuado para la ciberseguridad y las nuevas tecnologías.
9. **Dentro de lo posible, buscar la cooperación con los proveedores** y prestadores privados, interactuar con ellos y crear un clima de confianza que permita compartir información crítica sobre ciberseguridad.
10. **Asegurarse de que los contratos** con proveedores incluyan obligaciones, documentación y servicios de respuesta adecuados; también de que tengan claros los requisitos de seguridad, y verificar su cumplimiento.



### 3.3

## Decálogo para personal técnico de ciberseguridad y tecnologías de la información



### Nivel operativo

Las siguientes recomendaciones están dirigidas a quienes son responsables y están familiarizados con las tecnologías y sistemas por proteger en la ciudad. Se trata del personal que sigue las estrategias y las tácticas planificadas en los otros niveles y propone las directrices técnicas, de capacitaciones, y los procedimientos para la gestión, identificación, protección, detección, respuesta y recuperación frente a incidentes. El personal de TI suele ser el que asume la ciberseguridad, si bien en ocasiones se cuenta con expertos que tienen responsabilidades específicas en la materia. Las recomendaciones incluyen:

1. **Determinar el alcance** y los servicios y sistemas que hay que asegurar especialmente bajo la propia responsabilidad, y tener en claro cuáles son los órganos y actores de los que dependen.
2. **Conocer los lineamientos**, estrategias, políticas, normas y buenas prácticas definidos en la ciudad y hacerlos operativos en los sistemas de los cuales se es responsable.
3. **Participar y contribuir a la evaluación**, gestión y planificación de la ciberseguridad como un proceso continuo.
4. **Identificar los órganos y responsabilidades** específicas de ciberseguridad en la entidad en la que se trabaja, y conocer la responsabilidad de unos y otros ante incidentes y respuestas a los mismos.
5. **Realizar un proceso de autoevaluación** o diagnóstico del nivel de madurez de las capacidades de la ciudad según las herramientas de las que se disponga y, a partir de allí, dimensionar las capacidades y recursos necesarios.
6. **En la medida de las responsabilidades contraídas, planificar** y determinar los pasos concretos para cumplir con los objetivos.
7. **Proteger e implantar sistemas de identificación**, autenticación y control de acceso, así como mecanismos de detección de anomalías y vigilancia para dar respuesta a incidentes.
8. **Si se encuentra dentro de las competencias asignadas, vigilar que la adquisición de bienes y servicios de tecnología por parte de la ciudad incluya la seguridad y privacidad** en el diseño y por defecto. Estar al día con los nuevos métodos y herramientas de los atacantes. Actualizar y mejorar el estado del *hardware* y del *software*. Si es posible, optar por sistemas automatizados para la detección y respuesta ante amenazas. Si se encuentra dentro de las propias responsabilidades, estar a la vanguardia y crear equipos de seguridad ofensiva o activa para adelantarse a los ataques.
9. **Establecer los perfiles del equipo humano** que tendrá a cargo la función de ciberseguridad a partir de los roles definidos en los procesos y los procedimientos.
10. **Integrar las políticas de privacidad** y protección de datos con las de ciberseguridad.

# 4

## *Capacidades técnicas para brindar ciberseguridad a la ciudad*



Augusto Navarro

*«Dentro de los compromisos que deben asumirse, se encuentra el cumplimiento de las normas, políticas y lineamientos dispuestos para la función de ciberseguridad.»*



# 4

## Capacidades técnicas para brindar ciberseguridad a la ciudad



El lector o la lectora de esta guía ya han podido entender los peligros, ciberamenazas, actores, motivaciones, más el impacto que generan los ciberataques a las ciudades, y –con ello– la necesidad de tomarse en serio la ciberseguridad urbana desde hoy mismo. Para eso, ya cuentan con recursos, buenas prácticas y recomendaciones que les permitirán encarar la empresa. Ahora bien, la ciberseguridad entraña un componente técnico ineludible, y esta sección se dirige especialmente a los responsables y al personal de perfil tecnológico encargados de la ciberseguridad de la ciudad, a quienes se les facilita una hoja de ruta para la implementación de modelos de madurez de capacidades. Dentro de los compromisos que deben asumirse, se encuentra el cumplimiento de las normas, políticas y lineamientos dispuestos para la función de ciberseguridad (gráfico 4.1).

Gráfico 4.1.

### Lineamientos para el personal de ciberseguridad y tecnologías de la información

- 1 **Identificar** información asociada a los servicios y los activos de apoyo que se van a proteger.
- 2 **Cumplir** y ejecutar las normas y políticas dispuestas para la función de ciberseguridad; identificar el modelo de ciberseguridad por implementar.
- 3 **En el marco del modelo de ciberseguridad, definir** las capacidades por implantar; para ello, los procesos, la tecnología y la información deberán integrarse a la institucionalidad.
- 4 **Identificar** y valorar los datos críticos, así como los especialmente confidenciales para la ciudad.
- 5 **Establecer** los requisitos básicos de seguridad que se deben incorporar en el proceso de adquisición de productos y servicios de tecnologías seguros.
- 6 **Ejecutar** el plan de formación y comunicación de la iniciativa.
- 7 **Ejecutar** el plan de financiamiento, de acuerdo con la hoja de ruta trazada y los recursos asignados.

Fuente: Elaboración propia (2021).

El objetivo esencial de la hoja de ruta es implementar y fortalecer las capacidades, lo cual permite poner en marcha iniciativas a mediano y largo plazo. Las capacidades se definen sobre la base del modelo de madurez de capacidades en ciberseguridad que se elija (cuadro 4.1). En función de sus necesidades, el personal técnico puede optar por uno de los diferentes modelos de madurez existentes.

Cuadro 4.1.

## Modelos de madurez de ciberseguridad para organizaciones

Acrónimo	Nombre	Propuesto por	Niveles de madurez
CCSMM	Modelo de madurez de la ciberseguridad comunitaria	White	5
COBIT	Objetivos de control para la información y tecnología relacionada	ISACA	5
CSF-NIST	Marco de ciberseguridad	NIST	5
C2M2	Modelo de madurez de la capacidad de ciberseguridad	Curtis	4
ISMS	Sistema de gestión de la seguridad de la información - ISO/IEC 27001	ISO/IEC	5
ISM3	Sistema de gestión de seguridad de la información - Modelo de madurez	ISM3	5
-	Modelo de madurez de la capacidad de seguridad cibernética de NICE (Iniciativa Nacional para la Educación en Ciberseguridad)	US DHS	3
RMM	Modelo de gestión de la resiliencia	CERT	4
SSE-CMM	Modelo de capacidad de ingeniería de seguridad de sistemas	NSA	5

Fuente: Adaptado de Rea-Guaman et al. (2017).

El desarrollo y la implementación de capacidades técnicas se pueden resumir en una “función de ciberseguridad” que contempla **la gestión** (reingeniería de procesos y definición de funciones claves); la formación del personal, la capacitación y la gestión de cambios; **las actividades técnicas** (sistemas de información o *software* y la infraestructura que les da soporte o *hardware*); y, finalmente, **la gestión de la información** (que conecta los procesos con las TIC, las tecnologías digitales y las tecnologías emergentes). El personal de TI es el encargado de esta función de ciberseguridad, para lo cual debe seguir los tres pasos que se detallan a continuación: autoevaluación de capacidades, identificación de las capacidades que se deben desarrollar y operación de la función de ciberseguridad.






## 4.1

# Pasos de la función de ciberseguridad

Como ya se ha señalado, la función de ciberseguridad se desarrolla a partir de tres pasos (véase el gráfico 4.2).

Gráfico 4.2.

## Pasos por seguir para implantar la función de ciberseguridad

- 1  **Autoevaluación de capacidades**
- 2  **Identificación de capacidades para desarrollar**
- 3  **Operación de la función de ciberseguridad**

Fuente: Elaboración propia (2021).

**El primer paso** para **implantar la función de ciberseguridad** implica realizar un proceso de **autoevaluación** o diagnóstico del nivel de madurez de las capacidades, de acuerdo con los instrumentos propios del modelo elegido y la información asociada a los servicios y los activos de apoyo que se van a proteger. En el caso de esta guía, el autodiagnóstico se incluye a través del enlace [www.iadb.org/cibereval](http://www.iadb.org/cibereval), para lo cual se toma como referencia el modelo de ciberseguridad del NIST, que es uno de los más utilizados. Sin perjuicio de ello, cualquiera de los modelos o prácticas adoptados podrían utilizarse o combinarse en función de los servicios de la ciudad que se desee proteger.

Entre otros objetivos, el proceso de autoevaluación busca determinar el nivel de madurez a partir de las siguientes preguntas:

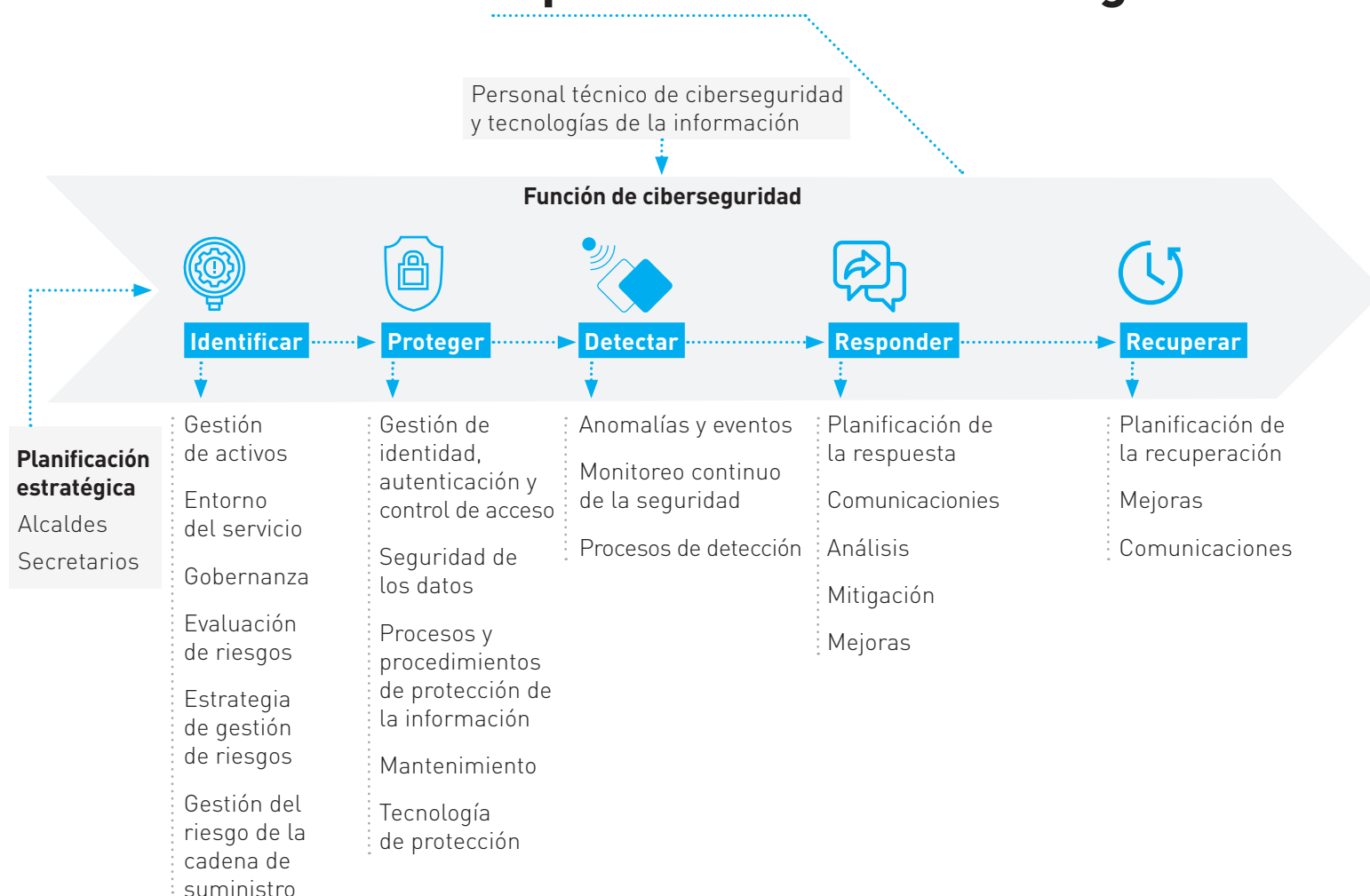
1. ¿Qué actividades se deben realizar?
2. ¿Qué información se utiliza o se produce en los procesos?
3. ¿Quiénes están involucrados en las capacidades?
4. ¿Qué tecnología debe dar sostén a dichas capacidades?

**El segundo paso** es la **identificación** de las capacidades que **debe desarrollar** la función de ciberseguridad a partir de los resultados conseguidos en el autodiagnóstico. La determinación de las capacidades estará vinculada con la identificación, protección, detección, respuesta y recuperación de incidentes que se puedan presentar en los servicios ofrecidos.



Gráfico 4.3.

## Identificación de capacidades en ciberseguridad



Fuente: Elaboración propia; modelado a partir del marco de ciberseguridad NIST, usando ArchiMate 3.10.

**El tercer paso** es la puesta en **operación** de la función de ciberseguridad. Como ejemplo, puede mencionarse el modelo marco de ciberseguridad del NIST, que corresponde a acciones específicas que apuntan a **cinco capacidades**: identificar, proteger, detectar, responder y recuperar, elementos que se despliegan con mayor detalle a continuación.

## 4.1.1 Identificar

Esta capacidad permite comprender el contexto en el que se desarrolla el servicio de la ciudad, los recursos que respaldan las funciones críticas y los riesgos de seguridad cibernética relacionados con la prestación de dicho servicio. Posibilita administrar el riesgo de seguridad cibernética de sistemas, personas, activos, datos y capacidades. A continuación, se presentan las subcapacidades que forman parte de esta capacidad, de acuerdo con las categorías propuestas por el NIST, para lo cual se toman como ejemplo los servicios financieros de una municipalidad.



### Identificar

- Gestión de activos
- Entorno del servicio
- Gobernanza
- Evaluación de riesgos
- Estrategia de gestión de riesgos
- Gestión del riesgo de la cadena de suministro

### Identificar:

**Los dispositivos** y sistemas físicos, plataformas de *software* y aplicaciones integradas a la gestión financiera de la ciudad.

**El hardware**, dispositivos, datos, tiempo, personal y *software*, en función de su clasificación, criticidad y valor integrados en los servicios financieros de la ciudad.

**La cadena de suministro** integrada en los servicios financieros.

**Los requisitos legales y regulatorios** con respecto a la protección de datos tratados en las transacciones económicas y financieras de la ciudad.

**Los impactos y las probabilidades** de que el servicio financiero sea afectado por un ataque informático.

**La estrategia de gestión de riesgos** para los servicios financieros a los que se brinda soporte.



## 4.1.2 Proteger

Abarca las subcapacidades que permiten desarrollar e implementar medidas de seguridad adecuadas para garantizar la provisión de los servicios urbanos. Incluye la capacidad de limitar o contener el impacto de un posible evento de seguridad cibernética.



### Proteger

Gestión de identidad, autenticación y control de acceso

Seguridad de los datos

Procesos y procedimientos de protección de la información

Mantenimiento

Tecnología de protección

### Realizar acciones de protección como las siguientes:

**Auditorías** de los dispositivos que son utilizados.

**Emisión** de identidades, credenciales y autorizaciones, para acceder a los servicios financieros de la ciudad.

**Capacitación** de usuarios vinculados a los servicios financieros de la ciudad.

**Mecanismos** de comprobación de la integridad para verificar el *software*, el *firmware* y la integridad de la información.

**Establecimiento** de procesos de control de cambios de la configuración de los sistemas que soportan toda la información financiera de la ciudad.

**Realización** y mantenimiento de copias de seguridad de la información.

**Establecimiento** y gestión de planes de respuesta frente a un ataque informático.

**Protección** de las redes de comunicaciones y control.

**Implementación** de mecanismos (por ejemplo, a prueba de fallas, equilibrio de carga, cambio en caliente o *hot swap*) para lograr los requisitos de resiliencia en situaciones normales y adversas.



### 4.1.3

## Detectar

Implica el desarrollo y la puesta en marcha de acciones apropiadas para identificar la ocurrencia de un evento de seguridad cibernética en los servicios de la ciudad.



#### Detectar

- Anomalías y eventos
- Monitoreo continuo de la seguridad
- Procesos de detección

#### Llevar a cabo acciones de detección como las siguientes:

**Recolectar** la información y analizar los ataques detectados para comprender los objetivos y métodos.

**Determinar** el impacto de los ataques.

**Monitorear** la actividad del personal, de los proveedores y de la red para detectar posibles eventos de seguridad cibernética.

**Establecer** mecanismos para detectar *software* no autorizado, código malicioso, entre otros.

**Aprobar** los procesos de detección.



#### 4.1.4

### Responder

Esta capacidad consiste en desarrollar e implementar mecanismos apropiados para tomar medidas con respecto a un incidente detectado de seguridad cibernética.



#### Responder

- Planificación de la respuesta
- Comunicaciones
- Análisis
- Mitigación
- Mejoras

**Poner en marcha actividades de respuesta como las siguientes:**

**Ejecutar** el plan de respuesta durante o después de un incidente.

**Comunicar** los incidentes a las autoridades y de acuerdo con el esquema de coordinación establecido por la institucionalidad.

**Investigar** las notificaciones de los sistemas de detección.

**Comprender** el impacto del incidente.

**Realizar** análisis forenses.

**Incorporar** las lecciones aprendidas en los planes de respuesta.

**Actualizar** las estrategias de respuesta frente al incidente.

**Contener** y mitigar los incidentes y vulnerabilidades identificados.

**Documentar** todo el proceso; incorporar las enseñanzas obtenidas y actualizar el plan de respuesta.





#### 4.1.5

### Recuperar

Esta capacidad comprende el desarrollo y la puesta en marcha de acciones apropiadas para mantener los planes de resiliencia y restablecer cualquier capacidad o servicio que se haya visto afectado debido a un incidente de seguridad cibernética.



#### Recuperar

- Planificación de la recuperación
- Mejoras
- Comunicaciones

**Deberían realizarse acciones de recuperación como las siguientes:**

**Ejecutar** el plan de recuperación durante o después de un incidente de seguridad cibernética ocasionado a los servicios financieros de la ciudad.

**Incorporar** las lecciones aprendidas a los planes de recuperación.

**Reparar** la reputación de la entidad afectada después del incidente.

**Comunicar** las actividades de recuperación a las partes interesadas internas y externas, así como también a los equipos ejecutivos y de administración.





## 4.2

# Tecnología de la función de ciberseguridad

La función de ciberseguridad puede requerir diferentes servicios de procesamiento de información, incluso servicios especializados de *hardware* y *software* para pruebas de penetración, servicios de monitoreo, de auditoría y de informática forense. Es conveniente optar por sistemas automatizados.



### 4.3

## Funciones del máximo responsable de ciberseguridad

El máximo responsable en este campo debe cumplir con las siguientes funciones:

- Informar a los responsables de la ciudad de todos los asuntos relacionados con la ciberseguridad y comunicarse con las autoridades competentes.
- Establecer el marco general de gobernanza y la política sobre ciberseguridad, que será revisada y aprobada por los líderes de alto rango, por lo menos una vez al año.
- Hacer acatar la política de seguridad de los activos y equipos, garantizar el cumplimiento normativo aplicable, supervisar la revisión anual de los documentos relativos a la seguridad de la información y los resultados de las auditorías.
- Hacer un inventario y tener una visión de la infraestructura tecnológica por proteger. Tomar decisiones de ciberseguridad de todos los productos, servicios, adquisiciones y desarrollo de aplicaciones internas de TI y tecnología operativa existentes.
- Ejecutar evaluaciones de impacto de seguridad y privacidad.
- Cooperar con los proveedores del sector privado y velar por la inclusión de la ciberseguridad en la contratación.
- Responsabilizarse de la capacitación para los funcionarios y realizar evaluaciones de la misma en forma anual.
- Examinar y registrar todos los incidentes de seguridad y adoptar las medidas necesarias de acuerdo con un plan específico de respuesta a incidentes y de recuperación ante desastres. Esta estrategia debe probarse, al menos una vez al año, para determinados sistemas.





5

## ***El BID y la ciberseguridad en las ciudades***



***«El BID, en tanto socio estratégico, busca apoyar a los países de la región para que puedan afrontar el nuevo desafío de la ciberseguridad urbana.»***



# 5

## El BID y la ciberseguridad en las ciudades



El Grupo BID ha definido la “Visión 2025: Reinvertir en Las Américas” como guía para apoyar a los países de ALC en la recuperación posterior a la pandemia. La visión se basa en cinco pilares de acción: 1) la transformación digital y la adopción más rápida de tecnologías en el sector público y privado, 2) el fortalecimiento de las cadenas de valor de la región, 3) el cambio climático, 4) el apoyo a las pymes, 5) la igualdad de género y la inclusión. Con ello, se busca impulsar oportunidades de crecimiento sostenible, reactivar la economía de la región, promover el progreso social y fortalecer la buena gobernanza.

Desde hace más de una década, el BID acompaña a la región en la transformación digital. A través del **Marco de Acción de Transformación Digital**,<sup>18</sup> se ha propuesto fortalecer la conectividad, la gestión pública digital, la transformación digital de los servicios sociales y de infraestructura, el desarrollo sostenible y la digitalización de las ciudades, además de la transformación digital del sector privado.

La transformación digital, y el uso de nuevas tecnologías y datos masivos contribuyen a la formulación de políticas públicas para responder a los principales desafíos sociales y lograr los Objetivos de Desarrollo Sostenible (ODS) formulados por las Naciones Unidas. La pandemia de COVID-19 aceleró la **transformación digital** de los países de la región, pero son las **ciudades** las que se enfrentan a un mayor desafío para garantizar la continuidad de la prestación de bienes y servicios a los ciudadanos.

La transformación de una ciudad hacia un modelo de gestión más inteligente, con tecnologías digitales, aumenta la vulnerabilidad de los activos en el ciberespacio.

**Por esto, la ciberseguridad es un tema emergente y crucial que concierne a la región y a todas las ciudades, y que adquiere creciente visibilidad en la agenda política subnacional, nacional, regional y mundial, enmarcada en un proceso de globalización de los sistemas informáticos y las cadenas de valor.**

.....  
18. El Marco mencionado se encuentra pendiente de aprobación al momento de publicarse este documento.

Por eso, el BID, en tanto socio estratégico, busca apoyar a los países de la región para que puedan afrontar el nuevo desafío de la ciberseguridad urbana.

**El Banco tiene alianzas estratégicas con los gobiernos más avanzados en materia digital, lo cual incluye la ciberseguridad; por ejemplo, Canadá, Estonia, España, Israel, Reino Unido y República de Corea, así como con socios clave del ámbito académico, el sector privado y los organismos de desarrollo, lo cual le facilita el acceso rápido al conocimiento y su intercambio.**



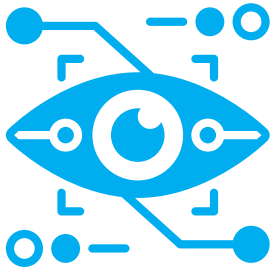
Adicionalmente, el equipo técnico del BID colabora con los equipos de los gobiernos beneficiarios y apoya una transformación digital adaptada a la realidad de cada país, área metropolitana o municipio.

El Banco cuenta con un equipo dedicado a brindar apoyo a los países de ALC en materia de ciberseguridad, el cual forma parte de la División de Innovación para Servir al Ciudadano (IFD/ICS). Desde el clúster de **Datos y Gobierno Digital** se diseñan proyectos para fortalecer la ciberseguridad a nivel nacional, o bien para reforzar las capacidades de ciberseguridad en sectores como transporte, salud, servicios financieros, seguridad ciudadana y gobierno digital, entre otros, de los que depende la ciudadanía. Además, se brinda apoyo en la formulación de políticas públicas de ciberseguridad, la formación de profesionales y la generación y el intercambio de conocimientos. Entre los estudios publicados por el equipo se destaca, como ya se ha señalado, el [Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe](#), realizado en colaboración con la OEA, el cual recoge las políticas y prácticas de ciberseguridad de los países de la región, su madurez cibernética, así como brechas y oportunidades para la acción en este campo.



A nivel subnacional, las ciudades de la región han registrado un crecimiento demográfico acelerado en las últimas décadas, con lo cual la transformación digital y la adopción de la tecnología para la prestación de bienes y servicios públicos han cobrado mayor relevancia.

**Por ende, la ciberseguridad urbana y municipal se ha convertido rápidamente en una temática fundamental que es menester atender de manera preventiva.**



En este ámbito, el grupo temático de **Ciudades Inteligentes y Datos Cívicos** de la División de Vivienda y Desarrollo Urbano (CDS/HUD) del Banco proporciona su apoyo para la transformación de las ciudades hacia un modelo de ciudades inteligentes y ciberseguras. A nivel local, la ciberseguridad crece en importancia a medida que se recurre cada vez más a la tecnología para la provisión de servicios y la gestión de la infraestructura física y digital.

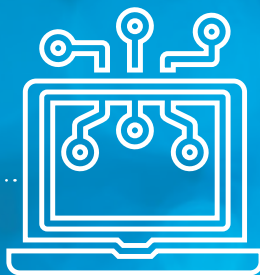
Para reducir la brecha de conocimiento en materia de transformación digital, el BID desarrolló estudios, proyectos piloto y herramientas de autoevaluación en ciberseguridad en sectores como energía y salud, a los cuales se suma ahora el ámbito específico de las ciudades ([www.iadb.org/cibereval](http://www.iadb.org/cibereval)). Esta herramienta ayudará tanto a conocer el nivel de prevención y preparación ante ciberataques como a definir futuras iniciativas de fortalecimiento de capacidades en las que el BID podrá proveer su respaldo para reforzar la ciberseguridad urbana.

Esperamos que esta *Guía de ciberseguridad para ciudades inteligentes* sea el punto de partida para comprender mejor la ciberseguridad, así como los riesgos e impactos potenciales, y difundir recomendaciones para transformar las 17.000 ciudades de la región en urbes más ciberseguras e inteligentes.





# Conclusiones



Las ciberamenazas están a la puerta de todas las ciudades, al acecho de cualquier vulnerabilidad tecnológica y humana. La ciberseguridad total no existe, pero son muchas las acciones que pueden ponerse en marcha en cada ciudad en particular para lograr la mayor protección posible.

Es cierto que para ello se requieren recursos, pero, como todo en la vida, lo que se necesita especialmente es una clara voluntad y el compromiso asumido por parte de los directivos y el personal de las ciudades, así como de las empresas que colaboran en ese ámbito.

Con esta guía no solo es posible conocer el problema sino también comenzar a abordarlo desde este mismo momento, de acuerdo con las capacidades con que se cuente y con la posición que se ocupe en la ciudad. Para que el entorno sea seguro y resiliente desde el punto de vista cibernético, esto es, para garantizar la prestación permanente de los servicios urbanos, hay que conocer el entorno que se va a proteger, el ecosistema y los actores participantes. Se debe entender que hay que gestionar los riesgos asociados a cada servicio. A partir de ahí, se trata de planificar las actividades, considerar la colaboración entre las partes, apuntar a la formación y capacitación permanente, obtener los recursos necesarios y determinar los pasos concretos por seguir. Hay que ser proactivo, tener clara disposición a cooperar con los actores involucrados, practicar y entrenar y capacitarse. Merece la pena.







# Referencias

- AEPD (Agencia Española de Protección de Datos). 2017. Código de buenas prácticas en protección de datos para proyectos *Big Data*. Madrid: AEPD. Disponible en: <https://www.aepd.es/es/media/guias/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf>.
- , 2018. Guía para Administraciones Locales. Madrid: AEPD. Disponible en: <https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf>.
- , 2019a. Guía Orientaciones y garantías en los procedimientos de anonimización de datos personales. Madrid: AEPD. Disponible en: <https://www.aepd.es/es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf>.
- , 2019b. Directrices para la elaboración de contratos entre responsables y encargados del tratamiento. Madrid: AEPD. Disponible en: <https://www.aepd.es/sites/default/files/2019-10/guia-directrices-contratos.pdf>.
- , 2020a. Adecuación al RGPD de tratamientos que incorporan inteligencia artificial: una introducción. Madrid: AEPD. Disponible en: <https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf>.
- , 2020b. Tecnologías y Protección de Datos en las AAPP. Madrid: AEPD. Disponible en: <https://www.aepd.es/es/media/guias/guia-tecnologias-admin-digital.pdf>.
- , 2020c. Webinario AEPD “Smart Cities: Más allá de la seguridad, la privacidad de los ciudadanos”. Madrid: AEPD. Disponible en: <https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/webinario-smart-cities>.
- , 2021. Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD. Madrid: AEPD. Disponible en: <https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf>.
- Agrafiotis, I. et al. 2018. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, Vol. 4(1), ty006. Disponible en: <https://doi.org/10.1093/cybsec/ty006>.
- Alianza Global de Ciudades Inteligentes del G-20. 2020. Política modelo. Política de rendición de cuentas de ciberseguridad. Tokio: World Economic Forum Centre for the Fourth Industrial Revolution Japan. Disponible en: <http://globalsmartcitiesalliance.org/wp-content/uploads/2020/12/Cyber-accountability-v1.2-ESP.pdf>.
- Alibasic, A., R. Al Junaibi, Z. Aung, W. Woon y M. I. Omar. 2017. Cybersecurity for Smart Cities: A Brief Review. *Lecture Notes in Computer Science*, 10097: 22-30. Disponible en: [https://www.researchgate.net/publication/312528431\\_Cybersecurity\\_for\\_Smart\\_Cities\\_A\\_Brief\\_Review](https://www.researchgate.net/publication/312528431_Cybersecurity_for_Smart_Cities_A_Brief_Review).
- Barrero, V. 2018. Estado de preparación en ciberseguridad del sector eléctrico en América Latina. Diagnóstico, recomendaciones y guía de buenas prácticas. Washington, D.C.: BID, Comisión de Integración Energética de la Comunidad, Govertis. Disponible en: <https://publications.iadb.org/publications/spanish/document/Estado-de-preparacion-en-ciberseguridad-del-sector-electrico-en-America-Latina.pdf>.
- BID (Banco Interamericano de Desarrollo) y OEA (Organización de los Estados Americanos). 2020. *Reporte ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe*. Washington, D.C.: BID. Disponible en: <https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf>.
- Biderman, C. et al. 2021. *Big Data* para el desarrollo urbano sostenible. Washington, D.C.: BID. <https://publications.iadb.org/pt/big-data-pa-ra-o-desenvolvimento-urbano-sustentavel>.
- BlueVoyant. 2020. State and local government security report. <https://www.bluevoyant.com/wp-content/uploads/2020/11/BlueVoyant-State-and-Local-Government-Report-26th-August-2020-FINAL.pdf>.
- Bouskela, M. et al. 2016. La ruta hacia las Smart Cities. Migrando de una gestión tradicional a la ciudad inteligente. Washington, D.C.: BID. Disponible en: <https://publications.iadb.org/es/la-ruta-hacia-las-smart-cities-migrando-de-una-gestion-tradicional-la-ciudad-inteligente>.
- CCN (Centro Criptológico Nacional). 2020. *Guía de Seguridad de las TIC*. CCN-STIC 803. ENS. Valoración de los sistemas. Madrid: Ministerio de Defensa. Disponible en: <https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/682-ccn-stic-803-valoracion-de-sistemas-en-el-ens-1/file.html>.
- Cerdeira, P. et al. 2020. Políticas públicas orientadas por datos: los caminos posibles para gobiernos locales. Washington, D.C.: BID. Disponible en: <https://publications.iadb.org/publications/spanish/document/Politicas-publicas-orientadas-por-datos-los-caminos-posibles-para-gobiernos-locales.pdf>, <http://dx.doi.org/10.18235/0002727>.



- Cerrudo, C., M. A. Asbini y B. Russell. 2015. Cyber Security Guidelines for Smart City Technology Adoption. *Securing Smart Cities*, pp. 1-17. Cloud Security Alliance (CSA). Disponible en: [https://securingsmartcities.org/wp-content/uploads/2016/03/Guidelines\\_for\\_Safe\\_Smart\\_Cities-1.pdf](https://securingsmartcities.org/wp-content/uploads/2016/03/Guidelines_for_Safe_Smart_Cities-1.pdf).
- CrowdStrike. 2021. *Global Threat Report*. Disponible en: <https://www.crowdstrike.com/resources/reports/global-threat-report-es>.
- CSIS (Center for Strategic & International Studies). 2021. Significant Cyber Incidents since 2006. Washington, D.C.: CSIS. Disponible en: [https://csis-website-prod.s3.amazonaws.com/s3fs-public/210804\\_Significant\\_Cyber\\_Events.pdf?bz-KYK94rq5\\_3lrbYVK4fcL0rmkNq6lNI](https://csis-website-prod.s3.amazonaws.com/s3fs-public/210804_Significant_Cyber_Events.pdf?bz-KYK94rq5_3lrbYVK4fcL0rmkNq6lNI).
- DHS/OCIA (Department of Homeland Security's Office of Cyber and Infrastructure Analysis). 2015. The future of smart cities: cyber-physical infrastructure risk. Washington, D.C.: DHA/OCIA. Disponible en: <https://us-cert.cisa.gov/ics/Future-Smart-Cities-Cyber-Physical-Infrastructure-Risk>.
- ECSO (European Cyber Security Organisation). 2018. *Smart cities and smart buildings sector report. Cyber security for the smart cities sector, WG3 Sectoral Demand*. Bruselas: ECSO. Disponible en: <https://ecs-org.eu/documents/publications/5fdb27182b472.pdf>.
- Efthymiopoulos, M-P. 2016. Cyber-security in smart cities: The case of Dubai. *Journal of Innovation and Entrepreneurship*, 5(11). Disponible en: [DOI 10.1186/s13731-016-0036-x](https://doi.org/10.1186/s13731-016-0036-x).
- Enerlis, Ernst and Young, Ferrovial y Madrid Network. 2012. *Libro Blanco Smart Cities*. 1ª edición. Disponible en: [http://www.innopro.es/pdfs/libro\\_blanco\\_smart\\_cities.pdf](http://www.innopro.es/pdfs/libro_blanco_smart_cities.pdf).
- ENISA (Agencia Europea de Seguridad de las Redes y de la Información). 2014. Secure ICT Procurement in Electronic Communications. Analysis and recommendations for procuring ICT securely in the Electronic Communications Sector. Heraclión: ENISA. Disponible en: [https://www.enisa.europa.eu/publications/secure-ict-procurement-in-electronic-communications/at\\_download/fullReport](https://www.enisa.europa.eu/publications/secure-ict-procurement-in-electronic-communications/at_download/fullReport).
- , 2015. Cyber security for Smart Cities. An architecture model for public transport. Heraclión: ENISA. Disponible en: <https://www.enisa.europa.eu/publications/smart-cities-architecture-model>.
- , 2020. Directrices sobre contratación para la ciberseguridad en los hospitales. Prácticas recomendadas para la seguridad de los servicios sanitarios. Heraclión: ENISA. Disponible en: <https://www.enisa.europa.eu/publications/report-files/translation-procurement-guidelines-for-cybersecurity-in-hospitals/procurement-guidelines-full-version-es.pdf>.
- Eurocities. 2016. EUROCITIES statement on the contractual public-private partnership on cybersecurity. Bruselas: Eurocities. Disponible en: [http://nws.eurocities.eu/MediaShell/media/EUROCITIES\\_cybersecurity\\_statement.pdf](http://nws.eurocities.eu/MediaShell/media/EUROCITIES_cybersecurity_statement.pdf).
- FEM (Foro Económico Mundial). 2021. Whitepaper, Governing Smart Cities: Policy Benchmarks for Ethical and Responsible Smart City Development. Ginebra: FEM y Deloitte. Disponible en: <https://www.weforum.org/whitepapers/governing-smart-cities-policy-benchmarks-for-ethical-and-responsible-smart-city-development>.
- Forrest, C. 2019. Vendor selection: what needs to be in a good policy. En: ZDNet-TechRepública, *A winning strategy for cybersecurity*. San Francisco, CA: CBS Interactive Inc. Disponible en: [http://book.itep.ru/depositary/security/surveys/SF\\_feb2019\\_cybersec.pdf](http://book.itep.ru/depositary/security/surveys/SF_feb2019_cybersec.pdf).
- Gagliardi, N. 2019. Electronic communications: what needs to be in a good policy. En: ZDNet-TechRepública, *A winning strategy for cybersecurity*. San Francisco, CA: CBS Interactive Inc. Disponible en: [http://book.itep.ru/depositary/security/surveys/SF\\_feb2019\\_cybersec.pdf](http://book.itep.ru/depositary/security/surveys/SF_feb2019_cybersec.pdf).
- García, M., D. Forscey y T. Blute. 2017. Beyond the Network: A Holistic Perspective on State Cybersecurity Governance. *Nebraska Law Review*, 96 (2).
- Gómez de Ágreda, Á. 2020. Ciberseguridad en ciudades. En: *Las ciudades: agentes críticos para una transformación sostenible del mundo*. Cuaderno de Estrategia 206. Madrid: Instituto Español de Asuntos Estratégicos. Disponible en: [http://www.ieee.es/publicaciones-new/cuadernos-de-estrategia/2020/Cuaderno\\_206.html](http://www.ieee.es/publicaciones-new/cuadernos-de-estrategia/2020/Cuaderno_206.html).
- Grupo del Artículo 29. 2011. Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes. Disponible en: <https://www.aec.es/conocimiento/documento/dictamen-13-2011-sobre-los-servicios-de-geolocalizacion-en-los-dispositivos-moviles-inteligentes/>.
- ICO (Information Commissioner Office). s.f. Anonymisation: managing data protection risk code of practice. Wilmslow: ICO. Disponible en: <https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf>.
- INCIBE (Instituto Nacional de Ciberseguridad). 2016. CEO, CISO, CIO... ¿Roles en ciberseguridad? León, España: INCIBE. Disponible en: <https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad>.

- INCIBE-OSI (Oficina de Seguridad del Internauta). s.f. *Guía de ciberataques*. León, España: INCIBE. Disponible en: <https://www.osi.es/es/guia-ciberataques>.
- Information System Authority. 2021. Three-level Baseline Security System ISKE. Tallin: República de Estonia. Disponible en: <https://www.ria.ee/en/cyber-security/it-baseline-security-system-iske.html>.
- Interpol (Organización Internacional de Policía Criminal). 2020. Panorama mundial de la ciberamenaza relacionada con la COVID-19. Madrid: Interpol. Disponible en: <https://www.interpol.int/es/Delitos/Ciberdelincuencia/Ciberamenazas-relacionadas-con-la-COVID-19>.
- IOActive. 2018. Smart Cities Cyber Security Worries. Seattle, WA: IOActive. <https://ioactive.com/wp-content/uploads/2018/10/IOActive-Smart-Cities-cybersecurity-worries.pdf>.
- ISO (Organización Internacional de Normalización). 2012. ISO/IEC 27032:2012: Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad. Ginebra: ISO. Disponible en: <https://www.iso.org/standard/44375.html>.
- . 2018. ISO/IEC 27005: Gestión de riesgos de la seguridad la información. Ginebra: ISO. Disponible en: <https://www.iso.org/standard/75281.html>.
- Kalinin, M. et al. 2021. Cybersecurity Risk Assessment in Smart City Infrastructures. *Machines*, 9, 78. Disponible en: <https://doi.org/10.3390/machines9040078>.
- La French Tech. 2019. C'est quoi La French Tech Rennes St Malo? Rennes St Malo: La French Tech. Disponible en: <https://lafrenchtech-rennes.fr/>.
- Mantelero, A. 2017. From group privacy to collective privacy: towards a new dimension of privacy and data protection in the Big Data era. En: L. Taylor, L. Floridi y B. van der Sloot (eds.), *Group privacy: new challenges of data technologies*. Dordrecht: Springer. Disponible en: <https://www.stiftung-nv.de/sites/default/files/group-privacy-2017-authors-draft-manuscript.pdf>.
- Martín, E. 2016. Smart Cities: El valor de construir ciudades inteligentes. *Revista TELOS*, 105. Disponible en: <https://telos.fundaciontelefonica.com/archivo/numero105/el-valor-de-construir-ciudades-inteligentes-con-ciberseguridad/>.
- MIAC (Ministry of Internal Affairs and Communications). 2020. *Smart City Security Guidelines*. Tokio: MIAC. Disponible en: [https://www.soumu.go.jp/main\\_sosiki/joho\\_tsusin/eng/presentation/pdf/Smart\\_City\\_Security\\_Guideline\\_ver1.0.pdf](https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/Smart_City_Security_Guideline_ver1.0.pdf).
- MINTIC (Ministerio de Tecnologías de la Información y las Comunicaciones). 2021. Modelo de Seguridad y Privacidad de la Información, v. 4.0. Bogotá: MINTIC. Disponible en: <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/>.
- Muñoz, M. et al. 2018. *Guía de Buenas Prácticas sobre Smart City para pequeños y medianos municipios*. Granada: Diputación de Granada, Red Granadina de Municipios hacia la Sostenibilidad (GRAMAS). Disponible en: <https://www.dipgra.es/uploaddoc/areas/349/SMARTCITY.pdf>.
- NCSC (National Counterintelligence and Security Center). 2021. *Insider Threat Mitigation for U.S. Critical Infrastructure Entities: Guidelines from an Intelligence Perspective*. Londres: NCSC. <https://www.dni.gov/files/NCSC/documents/news/20210319-Insider-Threat-Mitigation-for-US-Critical-Infrastru-March-2021.pdf>.
- New America, N. Cohen y B. Nussbaum. 2018. Cybersecurity for the States: Lessons from Across America. Washington, D.C.: Cybersecurity Initiative, New America. Disponible en: <https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-states-lessons-across-america>.
- . 2019. Smart is Not Enough. How to ensure the technologies of the future don't break our cities (and us with them). Washington, D.C.: Cybersecurity Initiative, New America. Disponible en: <https://www.jstor.org/stable/resrep19969.1>.
- NIST (Instituto Nacional de Estándares y Tecnología). 2008. *Guide for Mapping Types of Information and Information Systems to Security Categories*. Special Publication 800-60 Volume I, Revision 1. Gaithersburg, MD: NIST. Disponible en: [https://tsapps.nist.gov/publication/get\\_pdf.cfm?pub\\_id=152106](https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152106).
- . 2019. Smart and Secure Cities and Communities Challenge (SC3), GCTC-SC3 Cybersecurity and Privacy Advisory Committee Guidebook, Global City Teams Challenge 2019. Gaithersburg, MD: NIST. Disponible en: <https://www.nist.gov/publications/2019-global-city-teams-challenge-smart-and-secure-cities-and-communities-challenge-expo>.
- OCDE (Organización para la Cooperación y el Desarrollo Económicos). 2015. Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document. París: OCDE. Disponible en: <http://dx.doi.org/10.1787/9789264245471-en>.

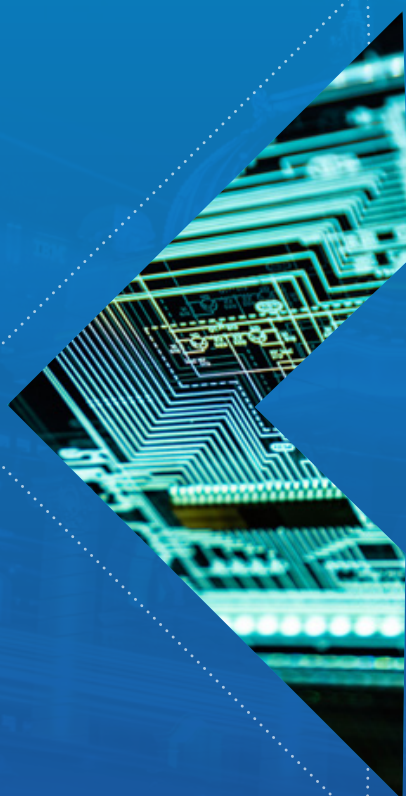
- OEA (Organización de los Estados Americanos). 2019. Clasificación de datos. White paper series. Washington, D.C.: OEA. Disponible en: <https://www.oas.org/es/sms/cicte/docs/ESP-Clasificacion-de-Datos.pdf>.
- OSPI (Observatorio del Sector Público). 2017. Ciberseguridad en el sector público. Documento de conclusiones. Disponible en: [https://www.ospi.es/export/sites/ospi/documents/informes/Informe\\_ciberseguridad.pdf](https://www.ospi.es/export/sites/ospi/documents/informes/Informe_ciberseguridad.pdf).
- Pandey, P. et al. 2020. Making smart cities cybersecure. Ways to address distinct risks in an increasingly connected urban future. Deloitte Insights. Disponible en: <https://www2.deloitte.com/us/en/insights/focus/smart-city/making-smart-cities-cyber-secure.html>.
- PwC. 2021. Global Digital Trust Insights Survey 2021. Cybersecurity comes of age. Londres: PwC. Disponible en: <https://www.pwc.com/gx/en/issues/cybersecurity/digital-trust-insights-2021.html>.
- Ranchordás S. y C. Goanta. 2020. The New City Regulators: Platform and Public Values in Smart and Sharing Cities. *Computer Law & Security Review*, 36. Disponible en: <https://doi.org/10.1016/j.clsr.2019.105375>.
- Razavi, A., S. Moschoyiannis y P. Krause. 2009. An open digital environment to support business ecosystems. *Peer-To-Peer Networking and Applications*, 2(4): 367-397. Disponible en: [DOI:10.1007/s12083-009-0039-5](https://doi.org/10.1007/s12083-009-0039-5).
- Rea-Guaman, Á. M., I. S. Sánchez-García, T. San Feliu Gilabert y J. A. Calvo-Manzano Villalón. 2017. Modelos de madurez en ciberseguridad: una revisión sistemática. En: 12ª Conferencia Ibéricas de Sistemas y Tecnologías de la Información, 21-24 de junio de 2017, Lisboa, Portugal, pp. 284-289.
- Salvador, C. 2021. Inteligencia artificial y gobernanza de datos en la administración pública: sentando las bases para su integración a nivel corporativo. En: R. Carles (coord.), *Repensando la Administración Pública. Administración digital e innovación pública*. Madrid: INAP. Disponible en: <https://www.libreriavirtuali.com/inicio/Administraci%C3%B3n-digital-e-innovaci%C3%B3n-p%C3%BAblica-Repensando-la-Administraci%C3%B3n-P%C3%BAblica-EB00K-p306540049>.
- Shacklett, M. 2019. 10 ways to develop cybersecurity policies and best practices. En: ZDNet-TechRepública, *A winning strategy for cybersecurity*. San Francisco, CA: CBS Interactive Inc. Disponible en: [http://book.itp.ru/depositary/security/surveys/SF\\_feb2019\\_cybersec.pdf](http://book.itp.ru/depositary/security/surveys/SF_feb2019_cybersec.pdf).
- Soare, S. y J. Burton. 2020. Smart Cities, Cyber Warfare and Social Disorder. CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence. Disponible en: [https://ccdcoe.org/uploads/2020/12/6-Smart-Cities-Cyber-Warfare-and-Social-Disorder\\_ebook.pdf](https://ccdcoe.org/uploads/2020/12/6-Smart-Cities-Cyber-Warfare-and-Social-Disorder_ebook.pdf).
- Stilgherrian. 2019. Security training is useless unless it changes behaviours. ZDNet-TechRepública, *A winning strategy for cybersecurity*. San Francisco, CA: CBS Interactive Inc. Disponible en: [http://book.itp.ru/depositary/security/surveys/SF\\_feb2019\\_cybersec.pdf](http://book.itp.ru/depositary/security/surveys/SF_feb2019_cybersec.pdf).
- Townsend, A. y P. Zambrano-Barragán. 2019. Big Urban Data. A Strategic Guide for Cities. Washington, D.C.: BID. Disponible en: [https://publications.iadb.org/publications/spanish/document/BIG\\_Data\\_urbana\\_Una\\_gu%C3%ADa\\_estrat%C3%A9gica\\_para\\_ciudades.pdf](https://publications.iadb.org/publications/spanish/document/BIG_Data_urbana_Una_gu%C3%ADa_estrat%C3%A9gica_para_ciudades.pdf).
- Trapenberg, F. et al. 2021. The Cybersecurity Risks of Smart City Technologies, What Do the Experts Think? UC Berkeley, CLTC White Paper Series. Disponible en: <https://cltc.berkeley.edu/2021/03/16/smart-cities>.
- UIT (Unión Internacional de Telecomunicaciones). 2008. Recomendación UIT-T X.1205 [04/2008]. Ginebra: UIT. Disponible en: <https://handle.itu.int/11.1002/1000/9136>.
- UNE (Asociación Española de Normalización). 2021. Comité CNT 178: Ciudades inteligentes. Madrid: UNE. Disponible en: <https://www.une.org/encuentra-tu-norma/comites-tecnicos-de-normalizacion/comite?c=CTN%20178>.



# Guía de *ciberseguridad*



para **ciudades inteligentes**



AUTORES: Lorenzo **Cotino**  
Marco **Sánchez**

EDITORES: Mauricio **Bouskela**  
Gilberto **Chona**  
Ariel **Nowersztern**  
Patricio **Zambrano-Barragán**  
Isabelle **Zapparoli**

