UNMSM
Fundación
SAN MARCOS
Por el desarrollo de la Ciencia y la Cultura

DIPLOMADO DE ESPECIALIZACIÓN

GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD

RESUMEN EJECUTIVO

Guía de ciberseguridad para ciudades inteligentes

JULIO – OCTUBRE 2026

CENCAEP
CAPACITA

RESUMEN EJECUTIVO

Guía de ciberseguridad para ciudades inteligentes

Enfoque ejecutivo y técnico para gobiernos locales y subnacionales

Documento fuente: Guía de ciberseguridad para ciudades inteligentes
Autores: Lorenzo Cotino y Marco Sánchez
Banco Interamericano de Desarrollo (BID), diciembre de 2021

Nota: la publicación original ya se encuentra en español. El presente documento realiza una síntesis ejecutiva, reorganizada y redactada en lenguaje profesional, sin incorporar contenidos ajenos a la fuente.

1. Propósito y visión ejecutiva

La transformación digital de las ciudades ha ampliado de manera sustancial la dependencia de redes, plataformas, sensores, dispositivos conectados, centros de operación, sistemas de información y datos. Este avance permite mejorar la prestación de servicios urbanos y la toma de decisiones, pero también incrementa la superficie de exposición frente a ciberataques. En este contexto, la ciberseguridad deja de ser un asunto exclusivamente tecnológico y se convierte en un componente de gobernanza, continuidad operativa, resiliencia urbana y protección de la ciudadanía.

La guía del BID está orientada a líderes de gobierno, gerentes municipales y personal de tecnologías de la información, incluyendo terceros que participan en la provisión de servicios. Su propósito es ayudar a las ciudades de América Latina y el Caribe a comprender los riesgos digitales, reducir la probabilidad de incidentes y limitar sus efectos cuando estos se materialicen.

Objetivo	Enfoque	Resultado esperado
Proteger a las ciudades en el ciberespacio	Gestión proactiva del riesgo y de los activos	Servicios e infraestructura más resilientes

Idea central

> **La ciberseguridad urbana debe anticipar los problemas, no limitarse a reaccionar cuando el daño ya se ha producido. La prevención, la preparación y la capacidad de recuperación deben incorporarse desde el diseño de la transformación digital.**

2. Riesgo cibernético en una ciudad inteligente

Una ciudad cibersegura debe proteger procesos, información y activos de apoyo: hardware, software, redes, personas, portales, instalaciones, estructuras organizativas, dispositivos conectados y servicios digitales. El ecosistema comprende a la ciudadanía, las plataformas de comunicación, la infraestructura tecnológica, los datos, los sensores y el conjunto de servicios públicos que dependen de ellos.

Los atacantes pueden perseguir motivaciones personales, empresariales, económicas, criminales o políticas. La guía destaca que las vulnerabilidades no provienen únicamente de fallas técnicas. También aparecen por debilidades de gobernanza, infraestructura obsoleta, ausencia de estrategias, deficiente gestión de riesgos e incidentes, falta de cooperación, dependencia de terceros y, de forma especialmente relevante, errores o carencias humanas.

Principales debilidades que elevan la exposición

- Ausencia de una estrategia integral y de una gobernanza clara de ciberseguridad.
- Políticas, normas y responsabilidades insuficientes o no implementadas.
- Falta de integración de proveedores, prestadores y cadena de suministro.
- Protección inadecuada de datos personales y datos críticos.
- Gestión insuficiente de vulnerabilidades, riesgos e incidentes.
- Software y hardware desactualizados, fallas técnicas y controles mal aplicados.
- Escasa capacitación, sensibilización y disponibilidad de perfiles especializados.
- Recursos financieros limitados y débil cooperación entre autoridades y sector privado.

3. Impacto de los ciberataques sobre la ciudad

Cuando un riesgo se materializa, puede comprometer datos, información, infraestructura y servicios esenciales. Los efectos trascienden el ámbito informático: una interrupción puede afectar transporte, emergencias, seguridad, salud, pagos, servicios municipales y otros componentes críticos de la vida urbana. Por ello, el impacto debe evaluarse en dimensiones operativas, sociales, económicas, políticas y reputacionales.

Dimensión	Consecuencia potencial
Operativa	Interrupción o degradación de servicios, sistemas y procesos municipales.
Económica	Costos de recuperación, indisponibilidad, reposición tecnológica y pérdida de productividad.
Social	Afectación directa a ciudadanos y servicios esenciales, incluida la seguridad pública.
Institucional	Pérdida de confianza, debilitamiento de la gobernabilidad y presión sobre responsables públicos.
Información y privacidad	Robo, exposición, alteración o indisponibilidad de datos, incluidos datos personales.

4. Hoja de ruta para la ciberseguridad urbana

La guía propone una hoja de ruta basada en gestión del riesgo. Su valor radica en ordenar la ciberseguridad como un proceso institucional continuo y no como una suma de soluciones aisladas. El punto de partida es conocer qué se debe proteger, quién interviene y cuáles son las dependencias tecnológicas y organizativas.

1. Identificar activos y actores: Inventariar servicios, información, datos, infraestructura, sistemas, dispositivos, personas, proveedores y dependencias.

2. Establecer la gobernanza: Integrar la ciberseguridad con la gobernanza de la ciudad inteligente y del dato; definir políticas, normas, competencias y prioridades.

3. Institucionalizar la función: Asignar liderazgo y responsabilidad a una persona, oficina o estructura con atribuciones y recursos definidos.

4. Proteger datos confidenciales y personales: Clasificar la información por riesgo y aplicar medidas proporcionales a su criticidad y sensibilidad.

5. Integrar a proveedores: Incorporar requisitos de seguridad, privacidad, respuesta, información y cumplimiento en contratación y cadena de suministro.

6. Formar, comunicar y concientizar: Construir una cultura de seguridad que alcance autoridades, directivos, empleados, técnicos, terceros y ciudadanía.

7. Financiar y transferir riesgos: Planificar recursos sostenibles para capacidades, renovación tecnológica y, cuando corresponda, seguros de ciberseguridad.

Gobernanza como condición habilitante

La gobernanza debe partir del cumplimiento legal y de la selección de estándares o modelos apropiados. La alta dirección debe fijar prioridades, tolerancia al riesgo y recursos; además, debe evitar vacíos de responsabilidad entre áreas. La coordinación con políticas nacionales y la participación en redes de cooperación fortalecen el intercambio de información y el acceso a buenas prácticas.

5. Factor humano, cultura y terceros

La guía concede al factor humano una importancia equivalente o superior a la de las medidas técnicas. La falta de conciencia, capacitación y comprensión del entorno digital facilita la ingeniería social y otros ataques. La cultura de seguridad debe comenzar en el alcalde y el concejo, extenderse a la alta dirección y alcanzar a todo el personal, técnicos, proveedores y ciudadanía.

La colaboración público-privada es igualmente crítica. Las ciudades dependen de prestadores de tecnología y servicios, por lo que la ciberseguridad debe formar parte del ciclo contractual: selección, requisitos de diseño, cumplimiento normativo, intercambio de información, atención de incidentes y verificación del desempeño. La confianza es necesaria, pero debe acompañarse de obligaciones claras y controles verificables.

6. Responsabilidades por nivel de gestión

Nivel	Responsabilidad principal	Prioridades
Estratégico Líderes de gobierno	Definir visión, políticas, institucionalidad y recursos.	Consenso político; liderazgo; normas; coordinación; financiamiento; renovación tecnológica; redes de cooperación.
Táctico Gerentes municipales	Convertir la política en planes, procesos y proyectos ejecutables.	Servicios a proteger; cumplimiento; procedimientos; datos críticos; formación; proveedores; recursos.
Operativo/Técnico TI y ciberseguridad	Implantar, operar y mejorar capacidades de protección.	Activos; controles de acceso; detección; respuesta; actualización; automatización; privacidad; autoevaluación.

Recomendaciones estratégicas prioritarias

- Tratar la ciberseguridad como una política de ciudad con continuidad más allá de un período de gobierno.
- Crear una institucionalidad con funciones, responsables y recursos claramente definidos.

- Evitar que políticas y planes queden solo en documentos: realizar pruebas, simulacros y evaluación continua.
- Incorporar seguridad y privacidad desde el diseño en adquisiciones, proyectos y servicios.
- Actualizar activos tecnológicos obsoletos y fortalecer mecanismos de automatización cuando sea viable.
- Planificar recursos financieros de corto, mediano y largo plazo para sostener las capacidades.
- Integrar al sector privado y participar en redes nacionales o regionales de ciberseguridad.

7. Capacidades técnicas para una ciudad cibersegura

La implementación técnica se concibe como una función de ciberseguridad que integra procesos, personas, tecnología e información. La guía propone tres pasos: autoevaluar el nivel de madurez, identificar las capacidades que deben desarrollarse y operar la función de manera continua.

Paso	Contenido
1. Autoevaluación	Determinar actividades, información utilizada, actores involucrados y tecnología que soporta las capacidades.
2. Identificación de capacidades	Definir brechas y capacidades necesarias a partir del diagnóstico y del modelo seleccionado.
3. Operación	Implantar y mantener capacidades para identificar, proteger, detectar, responder y recuperar.

Ciclo de capacidades inspirado en el marco NIST

Identificar. Comprender contexto, activos, servicios críticos, gobernanza, riesgos y dependencias de la cadena de suministro.

Proteger. Aplicar identidad, autenticación, control de acceso, seguridad de datos, procedimientos, mantenimiento y tecnologías de protección.

Detectar. Desarrollar monitoreo continuo, detección de anomalías, eventos y procesos de alerta.

Responder. Ejecutar planes de respuesta, comunicar, analizar, contener, mitigar, realizar análisis forense y documentar lecciones aprendidas.

Recuperar. Restablecer capacidades y servicios, mejorar planes y mantener comunicaciones durante la recuperación.

Modelos de madurez referenciados

La guía no impone un único modelo. Señala alternativas como COBIT, el Marco de Ciberseguridad del NIST, ISO/IEC 27001, C2M2, modelos CERT y otros esquemas de madurez. La selección debe responder a las necesidades, servicios y capacidades de cada ciudad, pudiendo combinarse prácticas cuando resulte pertinente.

Controles técnicos de especial relevancia

- Identificación, autenticación fuerte y control de acceso.
- Monitoreo continuo, detección de anomalías y vigilancia de eventos.

- Planes y procedimientos de respuesta y recuperación.
- Actualización y mantenimiento de hardware y software.
- Automatización de detección y respuesta cuando sea posible.
- Seguridad y privacidad desde el diseño y por defecto.
- Integración de protección de datos y ciberseguridad.
- Registro, documentación, análisis forense y aprendizaje posterior al incidente.

8. Protección de datos, información e inteligencia artificial

La seguridad de los datos debe aplicarse de acuerdo con su nivel de riesgo, con atención reforzada a información confidencial y datos personales. La gobernanza del dato y la ciberseguridad deben avanzar de manera coordinada. Esta integración es especialmente importante en ciudades que utilizan inteligencia artificial y tecnologías emergentes para monitorear, analizar o apoyar decisiones.

En el uso de inteligencia artificial, la guía destaca la necesidad de controles sobre calidad de datos, sesgos, robustez, registros de funcionamiento, trazabilidad, transparencia, explicabilidad, monitoreo y auditoría. El principio subyacente es que la innovación urbana debe desplegarse con garantías de seguridad, privacidad y control.

9. Financiamiento y sostenibilidad

La ciberseguridad requiere financiamiento planificado. Postergar inversiones puede elevar los costos cuando ocurre un incidente y dificultar la renovación de infraestructura obsoleta. La planificación debe cubrir recursos humanos, herramientas, tecnología, capacitación, pruebas, continuidad y respuesta. La guía también contempla los seguros como un mecanismo posible de transferencia de determinados riesgos, sin sustituir las medidas preventivas.

10. Conclusiones ejecutivas

La principal conclusión es que una ciudad inteligente no puede considerarse madura si su digitalización no está acompañada por capacidades de ciberseguridad. La conectividad, el Internet de las cosas, la inteligencia artificial y la explotación intensiva de datos generan valor público, pero también crean dependencias y nuevas superficies de ataque.

- La ciberseguridad debe formar parte de la agenda de gobierno y de la planificación estratégica de la ciudad.
- La gestión debe comenzar por conocer activos, servicios, actores, datos, dependencias y riesgos.
- La gobernanza requiere liderazgo visible, competencias claras, institucionalidad y coordinación con políticas nacionales.
- La prevención debe complementarse con detección, respuesta, recuperación y mejora continua.
- El factor humano exige capacitación permanente y una cultura compartida de seguridad.
- Los proveedores y la cadena de suministro deben integrarse formalmente a los requisitos y controles de ciberseguridad.
- La protección de datos y la privacidad deben integrarse con la seguridad digital desde el diseño.

- La inversión debe ser sostenida y orientada a capacidades, no únicamente a herramientas tecnológicas.
- La cooperación y el intercambio de información son indispensables para elevar la resiliencia urbana.

En síntesis, la guía plantea una visión de ciberseguridad basada en conocimiento del entorno, planificación, prevención proactiva, vigilancia constante, cooperación y capacitación permanente. Estas condiciones permiten aprovechar las tecnologías disruptivas sin comprometer la continuidad de los servicios, la información, la privacidad ni la confianza ciudadana.

11. Prioridades de implementación para la alta dirección

Prioridad	Acción inmediata	Resultado
1	Designar responsable y esquema de gobernanza.	Responsabilidad y coordinación claras.
2	Inventariar servicios, activos, datos y terceros críticos.	Visibilidad de la superficie de riesgo.
3	Realizar autoevaluación de madurez y riesgos.	Brechas priorizadas y hoja de ruta.
4	Aprobar políticas, procedimientos y requisitos contractuales.	Controles institucionalizados.
5	Implantar formación, simulacros y gestión de incidentes.	Mayor preparación y capacidad de respuesta.
6	Definir financiamiento y seguimiento periódico.	Sostenibilidad y mejora continua.

Fuente base

Cotino, L. y Sánchez, M. (2021). Guía de ciberseguridad para ciudades inteligentes. Banco Interamericano de Desarrollo.