Junio de 2024

Comunicaciones de vital importancia para la seguridad pública: ¿Se trata de infraestructura crítica?

En este documento se destaca la forma en que se tratan las comunicaciones de emergencia en función de la infraestructura crítica en diversas jurisdicciones. Ha sido elaborado por la Coalición Colaborativa para la Seguridad Pública Internacional (CC:IPS, por su acrónimo en inglés) cuyos integrantes se han comprometido a promover, apoyar y mejorar los servicios de comunicaciones de emergencia utilizando las tecnologías, normas y mejores prácticas más actualizadas y comúnmente aceptadas.

Declaración general

Nuestro objetivo es brindar a los profesionales de la seguridad pública de todo el mundo información que les permita entender la naturaleza y papel crítico de las comunicaciones de emergencia, incluidos los sistemas de llamadas de emergencia de tres dígitos (por ejemplo, 000/112/911/999), en el marco de sus propias infraestructuras críticas nacionales. Un documento como el presente en el que se comparten las posturas de varios países constituye un primer paso importante para que otros puedan comparar su propia posición e implicaciones.

Objetivo de este documento

Comprender dónde se reconocen y protegen las comunicaciones críticas en la legislación como un "ecosistema" que incluye la infraestructura crítica y los recursos humanos que en conjunto proporcionan las capacidades que las entidades encargadas de la seguridad pública necesitan para responder y proteger vidas y bienes materiales de una manera que satisfaga las expectativas del público y las de seguridad salud y bienestar de los primeros respondientes.

El objetivo de este documento es brindar información sobre la forma en que los distintos Gobiernos manejan los sistemas y las infraestructuras de comunicaciones críticas. No pretende ofrecer recomendaciones; más bien lo que se pretende es que el lector utilice la información como una investigación de base.

La definición de infraestructura crítica difiere de una jurisdicción a otra. Por ejemplo, en Australia las infraestructuras críticas son "aquellas instalaciones físicas, cadenas de suministro, tecnologías de la información y redes de comunicación, que en caso de que se destruyan, degraden o dejen de estar disponibles durante un período prolongado, impactaría significativamente el bienestar social o económico de la nación o afectarían su capacidad para realizar actividades de defensa y garantizar la seguridad nacional".

Resumen de los hallazgos

Los sistemas de llamadas de emergencia tienen diversos grados de complejidad en función de sus numerosos componentes. Sobre esta base, las organizaciones (es decir, Gobiernos, entidades de servicios de emergencia, etc.) que estén considerando designar ciertas partes de la infraestructura crítica, deben considerar cuidadosamente aspectos clave como la existencia de puntos únicos de falla y los actores que son clave para ellas.

Diferentes jurisdicciones opinan que los sistemas de llamadas de emergencia deben ser considerados como parte de la infraestructura crítica; sin embargo, este no siempre es el caso.

Los hallazgos a las que se ha llegado en este documento se resumen en el cuadro siguiente. La información se basa en los datos disponibles en el momento de la investigación.

País	Resumen
Australia	Las comunicaciones de emergencia NO se consideran como infraestructura crítica.
Canadá	La infraestructura 911 SÍ se le considera infraestructura crítica, pero no así las comunicaciones de emergencia.
Unión Europea	Las comunicaciones de emergencia NO se consideran como infraestructura crítica. Sin embargo, las instalaciones necesarias para facilitar esas comunicaciones (es decir, redes y servicios de comunicaciones electrónicas) SÍ se las considera como infraestructura crítica/servicios esenciales en la legislación de la Unión Europea. Dado que están incluidas en una directiva general para toda la Unión Europea (con un reglamento complementario en el que se definen los servicios esenciales), deben incorporarse a la legislación nacional de los Estados miembros.
Nueva Zelanda	Las comunicaciones de emergencia NO se consideran como infraestructura crítica.
Reino Unido	Las comunicaciones relativas a la seguridad pública NO se las considera como infraestructura crítica (la actual red nacional de comunicaciones críticas Airwave TETRA y la futura Red de Servicios de Emergencia basada en 4G LTE).
EE. UU.	Las comunicaciones de emergencia y el 911 SÍ son consideradas como infraestructuras críticas en dos de los 16 sectores de infraestructuras críticas cuyos activos, sistemas y redes (ya sean físicos o virtuales) son considerados vitales para Estados Unidos. Esos dos sectores son los servicios de emergencia y el sector de comunicaciones.
América Latina	En los casos de Ecuador y Costa Rica, la ciberseguridad y las infraestructuras críticas están estrechamente vinculadas, y la seguridad pública es uno de los pilares clave en Ecuador.

Otras consideraciones: inteligencia artificial

Al realizar la investigación para este documento ha quedado en claro que las infraestructuras críticas, la ciberseguridad y ahora la inteligencia artificial deben considerarse como un conjunto "vinculado" de iniciativas.

Por ejemplo, el 20 de diciembre de 2023, la Comisión Federal de Comunicaciones de Estados Unidos anunció que había constituido el noveno Consejo de Seguridad, Fiabilidad e Interoperabilidad de las Comunicaciones (CSRIC IX) con un grupo de trabajo que se encargaría de examinar la forma en que la inteligencia artificial y el aprendizaje automático pueden ser

utilizados para mejorar la seguridad, la confiabilidad y la integridad de las redes de comunicaciones de forma no discriminatoria, transparente y socialmente responsable. El CSRIC estará copresidido por la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA).

Hallazgos por país

En el resto de este documento se examinan los hallazgos país por país y, en donde fue posible, se incluyeron los enlaces a la documentación de las fuentes consultadas.

1. Australia

Como parte de la Estrategia de Ciberseguridad de Australia 2020[1], el Gobierno australiano introdujo reformas en la ley de infraestructuras críticas con el objetivo de proteger y mejorar aún más la resiliencia de estas.

La estrategia antes mencionada está siendo revisada actualmente para cubrir el período 2023-2030[2] y puede dar lugar a una nueva revisión de la legislación relacionada. Las consultas públicas para esta revisión se cerraron el 15 de abril de 2023 y el Centro para la Gestión de Desastre y Seguridad Pública (CDMPS, por su acrónimo en inglés) de la Universidad de Melbourne realizó la presentación.

La Comisión Parlamentaria Mixta de Inteligencia y Seguridad del Gobierno Federal[3] es responsable de la legislación pertinente a las infraestructuras críticas y la seguridad nacional. La legislación clave es la Ley sobre Seguridad de las Infraestructuras Críticas (Ley SOCI) de 2018[4] que incluye la creación de la categoría de "sistema de relevancia nacional"[5] que puede ser declarada por el Ministro del Interior.

En la Ley SOCI se identifican los siguientes 11 sectores de infraestructura crítica y clases de activos dentro de esos sectores

- Comunicaciones
  - Un activo de telecomunicaciones crítico
  - Un activo de radiodifusión crítico
  - Un sistema de nombres de dominio crítico
- Almacenamiento o tratamiento de datos
- Industria de defensa
  - Un activo crítico de la industria de defensa
- Energía
  - Un activo eléctrico crítico
  - Un activo de gas crítico
  - Un activo crítico de operadores del mercado energético
  - Un activo crítico de combustible líquido
- Servicios y mercados financieros
  - Un activo bancario crítico

1. https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf
2. 2023-2030 Australian Cyber Security Strategy Discussion Paper (homeaffairs.gov.au)
3. Parliamentary Joint Committee on Intelligence and Security – Parliament of Australia (aph.gov.au)
4. Security of Critical Infrastructure Act 2018 (legislation.gov.au)
5. Systems of National Significance and Enhanced Cyber Security Obligations Legislative Handbook (cisc.gov.au)

  - Un activo crítico del sistema de jubilación
  - Un activo crítico del sistema de seguros
  - Un activo crítico de la infraestructura del mercado financiero
- Alimentación y abastecimiento
  - Un activo crítico de alimentos y abastecimiento
- Atención de la salud y servicios médicos
  - Un hospital crítico
- Enseñanza superior e investigación
  - Un activo crítico del sistema educativo
- Tecnología espacial
- Transportes
  - Un puerto crítico
  - Un activo crítico de la infraestructura para el transporte de carga
  - Un activo crítico de los servicios de transporte de carga
  - Un activo crítico del transporte público
  - Un activo crítico de la aviación
- Agua y alcantarillado
  - Un activo crítico para el suministro de agua

La Ley SOCI se modificó en 2021 con el fin de que la gestión de riesgos, la preparación, la prevención y la resiliencia sean habituales para los propietarios y operadores de activos de infraestructuras críticas y mejorar el intercambio de información entre la industria y el Gobierno para entender mejor las amenazas.

Además de la Ley SOCI, la Ley de Enmienda de la Legislación de Telecomunicaciones y Otras 2017 —conocida como Reformas de Seguridad del Sector de las Telecomunicaciones— creó un marco regulatorio para gestionar mejor los riesgos de seguridad nacional vinculados al espionaje, sabotaje e interferencia extranjera en las redes e instalaciones de telecomunicaciones de Australia.

En Australia, las entidades gubernamentales clave responsables de las infraestructuras críticas, la ciberseguridad y la gestión de emergencias son el Ministerio del Interior[6], el Centro de Seguridad Cibernética e Infraestructura (CISC, por su acrónimo en inglés)[7] y la Agencia Nacional de Gestión de Emergencias[8]. Una referencia clave es el Plan Estratégico SAFECOM 2023.[9]

Con el fin de reconocer la importancia de las infraestructuras críticas, en noviembre de 2023 el CISC anunció que el mes de noviembre de cada año sería designado como el Mes de la Seguridad de las Infraestructuras Críticas en Australia. En esa línea, el 1 de noviembre de 2023, el Ministerio del Interior publicó la primera Evaluación Anual de Riesgos de Infraestructuras Críticas del CISC[10]. En esa evaluación[11] se resumen los posibles riesgos de seguridad a los que pueden enfrentarse los proveedores de infraestructuras críticas de Australia. Además, el 13 de

6. Department of Home Affairs
7. Cyber and Infrastructure Security Centre (cisc.gov.au)
8. National Emergency Management Agency (nema.gov.au)
9. SAFECOM Strategic Plan, March 2023 (cisa.gov)
   Recursos adicionales: Submission to Australia's 2023-2030 Cyber Security Strategy - 15 April 2023 (FINAL).pdf
10. https://www.cisc.gov.au/news-media/archive/article?itemId=1132
11. Critical Infrastructure Annual Risk Review First Edition 2023 (cisc.gov.au)

noviembre de 2023, el Ministro del Interior anunció que las "telecomunicaciones" serían reconocidas como "infraestructuras críticas" y afirmó que "estas normas, francamente, debieron haber estado en vigor hacía años".

Al anunciar esta decisión, el Ministro también dijo que las empresas de telecomunicaciones quedarían sujetas a la Ley SOCI, que les permitiría someterse a los nuevos estándares de buenas prácticas mundiales, comprometiéndolas a cumplirlos.

La consulta pública sobre la nueva reforma de la Ley SOCI comenzará a finales de enero de 2024.

2. Canadá

En Canadá, las infraestructuras críticas son aquellos "procesos, sistemas, instalaciones, tecnologías, redes, activos y servicios esenciales para la salud, la seguridad, la protección o el bienestar económico de los canadienses y el funcionamiento eficaz del Gobierno. Las infraestructuras críticas pueden ser independientes o estar interconectadas y ser interdependientes dentro y fuera de las provincias, territorios y fronteras nacionales. Cualquier perturbación en las infraestructuras críticas podrían provocar pérdidas catastróficas de vidas humanas, efectos económicos adversos y daños significativos a la confianza pública".

El Gobierno de Canadá utiliza un enfoque basado en los riesgos para reforzar la resiliencia de los activos y sistemas vitales de Canadá, como lo es el suministro de alimentos, la red de suministro eléctrico, el transporte, las comunicaciones y los sistemas de seguridad pública.

- En la Estrategia Nacional[12] se establece un enfoque de colaboración, federal-provincial-territorial y del sector privado, construido en torno a esquemas asociativos, gestión de riesgos e intercambio de información y protección.
- El Plan de Acción[13] representa el plan de implementación de la estrategia para mejorar la resiliencia de las infraestructuras críticas de Canadá.

La estrategia nacional se refiere a la seguridad de todos los canadienses, pero no menciona las comunicaciones de emergencia.

Dado que las catástrofes suelen ocurrir a nivel local, en la estrategia nacional de Canadá se reconoce que, en caso de emergencia, la primera respuesta casi siempre la darán los propietarios y operadores, el municipio o la provincia/territorio. El Gobierno federal cumple sus responsabilidades de líder a nivel nacional en materia de gestión de emergencias, respetando la legislación y competencias federales, provinciales y territoriales existentes. También es responsable de ayudar a las provincias/territorios cuando solicitan ayuda. La estrategia nacional se basa en el reconocimiento de que la mejora de la resiliencia de las infraestructuras críticas puede lograrse mediante la adecuada combinación de medidas de seguridad para hacer frente a incidentes intencionales y accidentales, prácticas de continuidad de las actividades para hacer frente a perturbaciones y mantener la continuidad de los servicios esenciales y la planificación de la gestión de emergencias para garantizar que existan procedimientos de respuesta adecuados para hacer frente a perturbaciones imprevistas y desastres naturales.

En esa estrategia se reconoce que la responsabilidad principal de reforzar la resiliencia de las infraestructuras críticas recae en los propietarios y operadores. Los niveles de Gobierno federal,

12. *National Strategy*
13. *Action Plan*

provincial y territorial también protegen sus propias infraestructuras críticas y apoyan a los propietarios y operadores para hacer frente a este desafío.

Lista de 10 sectores de Canadá:

- Energía y servicios públicos
- Finanzas
- Alimentación
- Transporte
- Gobierno
- Tecnologías de la información y la comunicación
- Salud
- Agua
- Seguridad
- Manufactura

3. Unión Europea

En la Directiva (UE) 2022/2557 relativa a la resiliencia de las entidades críticas se define el término infraestructura crítica como "un elemento, instalación, equipo, red o sistema, o parte de un elemento, instalación, equipo, red o sistema, que es necesario para la prestación de un servicio esencial". En esa misma directiva, un servicio esencial se define como "un servicio que es crucial para el mantenimiento de funciones sociales vitales, las actividades económicas, la salud pública y la seguridad, o el medio ambiente".

A continuación, figura la lista de entidades críticas enumeradas en el anexo de la Directiva (UE) 2022/2557. Además, en el Reglamento Delegado (UE) 2023/2450 de la Comisión, que complementa la Directiva (EU) 2022/2557, se profundiza en la definición de una lista no exhaustiva de servicios esenciales. Los servicios esenciales pertinentes para las comunicaciones de emergencia se enumeran a continuación bajo el rubro de entidades críticas pertinentes [del anexo de la Directiva (UE) 2022/2557]:

1. Energía
   - Electricidad
   - Sistemas urbanos de calefacción y de refrigeración
   - Crudo
   - Gas
   - Hidrógeno
2. Transporte
   - Transporte aéreo
   - Transporte por ferrocarril
   - Transporte marítimo y fluvial
   - Transporte por carretera
   - Transporte público
3. Banca
4. Infraestructura de los mercados financieros
5. Sanidad
6. Agua potable

7. Aguas residuales
8. Infraestructura digital

   (Lista no exhaustiva de servicios esenciales del Reglamento Delegado (UE) 2023/2450 en el rubro infraestructura digital)

   - Proveedores de puntos de intercambio de internet
   - Proveedores de servicios de DNS, excluidos los operadores de servidores raíz
   - Registros de nombres de dominio de primer nivel
   - Proveedores de servicios de computación en nube
   - Proveedores de servicios de centro de datos
   - Proveedores de redes de distribución de contenidos
   - Prestadores de servicios de confianza
   - Proveedores de redes públicas de comunicaciones electrónicas
   - Proveedores de servicios de comunicaciones electrónicas
9. Administración pública
10. Espacio
11. Producción, transformación y distribución de alimentos

Las entidades críticas incluidas en el ámbito de aplicación de esta legislación están sujetas a medidas de gestión de riesgos de ciberseguridad y a obligaciones de información en virtud de la Directiva (UE) 2022/2555 (Directiva SRI 2). La directiva también se aplica a:

1. Servicios postales y de mensajería
2. Gestión de residuos
3. Fabricación, producción y distribución de sustancias y mezclas químicas
4. Producción, transformación y distribución de alimentos
5. Fabricación
   - Fabricación de productos sanitarios y productos sanitarios para diagnóstico *in vitro*
   - Fabricación de productos informáticos, electrónicos y ópticos
   - Fabricación de material eléctrico
   - Fabricación de maquinaria y equipo no comprendido en otras partes
   - Fabricación de vehículos de motor, remolques y semirremolques
   - Fabricación de otro material de transporte
6. Proveedores de servicios digitales
7. Investigación

El artículo 108 del Código Europeo de Comunicaciones Electrónicas [Directiva (UE) 2018/1972] dice lo siguiente: “Los Estados miembros tomarán todas las medidas necesarias para garantizar la mayor disponibilidad posible de los servicios de comunicaciones vocales y de acceso a internet a través de las redes públicas de comunicaciones electrónicas en caso de fallo catastrófico de la red o en casos de fuerza mayor. Los Estados miembros velarán por que los proveedores de servicios de comunicaciones vocales adopten todas las medidas necesarias para garantizar el acceso sin interrupciones a los servicios de emergencia y la transmisión ininterrumpida de las alertas públicas”.

Nota: Una “directiva” es un acto legislativo con el que se establece un objetivo que los Estados miembros de la UE deben alcanzar. Sin embargo, corresponde a cada Estado miembro elaborar

sus propias leyes para alcanzar ese objetivo. Las directivas son vinculantes para los Estados miembros, pero están redactadas de tal manera que dan cierta flexibilidad a los Estados para aplicarlas de la manera que mejor se adapte a sus propias circunstancias nacionales (es decir, la puesta en práctica de la directiva europea mediante una legislación a nivel nacional).

Rumania

La red 112 de Rumania cuenta con:

- Fuentes de alimentación ininterrumpida para equipos
- El suministro eléctrico para los centros de respuesta de seguridad pública se origina en dos centrales diferentes de la red nacional, que actúan como medios primario y secundario de fuentes de energía y un generador eléctrico con un mínimo de 24 horas de autonomía sin recarga del depósito como contingencia
- Para garantizar la continuidad operativa del servicio 112, se aplican las siguientes medidas adicionales en caso de fallas en distintos condados:
    - Activación de rutas de reserva para otro centro de respuesta de seguridad pública del condado
    - Gestión de llamadas por operadores de otros centros de respuesta de seguridad pública
    - Activación técnica y operativa de centros de respaldo situados en lugares distintos del centro de respuesta de seguridad pública afectado
    - Enrutamiento automático o manual (mediante reconfiguraciones específicas) de llamadas/comunicaciones de emergencia a otro centro de respuesta de seguridad pública

En las infraestructuras de los operadores públicos, las medidas adoptadas en caso de corte del suministro eléctrico son específicas de las políticas del operador y no tienen carácter obligatorio en el ámbito nacional, pero se aplican los siguientes aspectos generales:

- Los centros de comunicaciones están ocupados con sistemas de alimentación ininterrumpida/centrales de alimentación/baterías que, en función de su importancia en la arquitectura de sus redes, proporcionan horas de autonomía.
- Dependiendo de la situación y prioridades para realizar la intervención, los equipos sobre el terreno pueden instalar generadores de energía móviles.
- Dependiendo de la situación y de las necesidades específicas, se toman medidas específicas para reducir el consumo de energía, por ejemplo:
    - Cerrando algunos servicios (es decir, apagando algunos equipos 2G que consumen mucha energía)
    - Cerrando algunos sitios cuyos servicios pueden ser ofrecidos por otros (en función de la carga y la importancia)

Alemania

En Alemania, los centros de respuesta de seguridad pública se consideran infraestructuras críticas. Todos están equipados con sistemas de energía de respaldo. En general, los centros de respuesta de seguridad pública dispondrán de un generador diésel y de suministros de combustible que permitan su funcionamiento durante varios días. Sírvase encontrar más información en BBK (Oficina Federal de Protección Civil y Ayuda en Casos de Desastres).

Reino de los Países Bajos

Puede encontrar información sobre las infraestructuras críticas de los Países Bajos en la ficha del Ministerio de Justicia y Seguridad. La "comunicación con y entre varios servicios de emergencia a través del número 112" figura en la categoría de infraestructuras críticas en los Países Bajos.

4. Reino Unido

La información que se presenta a continuación procede del sitio web de la Oficina Nacional Técnica para la Seguridad Física y Protección del Personal del Gobierno del Reino Unido (https://www.npsa.gov.uk/critical-national-infrastructure-0).

En el Reino Unido la definición de infraestructuras críticas es tal que no todo lo que está dentro del sector de la infraestructura nacional se considera "crítico". La definición oficial de infraestructuras críticas en el Reino Unido es la siguiente:

"*Aquellos elementos críticos de la infraestructura (a saber, activos, instalaciones, sistemas, redes o procesos y los trabajadores esenciales que los operan y facilitan), cuya pérdida o puesta en peligro podría dar lugar a:*

a) Un impacto perjudicial importante en la disponibilidad, integridad o prestación de servicios esenciales —incluidos aquellos servicios cuya integridad, en caso de verse comprometida, podría ocasionar una pérdida significativa de vidas o víctimas—, considerando impactos económicos o sociales significativos; o

b) Un impacto significativo en la seguridad nacional, la defensa nacional o el funcionamiento del Estado."

Las infraestructuras nacionales son aquellas instalaciones, sistemas, lugares, información, personas, redes y procesos necesarios para el funcionamiento de un país y de los que depende la vida cotidiana. Incluye también algunas funciones, lugares y entidades que no son críticos para el mantenimiento de los servicios esenciales, pero que requieren protección debido al potencial peligro para el público (centrales nucleares y plantas civiles de productos químicos, por ejemplo).

En el Reino Unido existen 13 sectores de infraestructura, cada uno de los cuales cuenta con uno o varios departamentos gubernamentales responsables del sector y de garantizar la seguridad de los activos críticos. Estos sectores son los siguientes:

- Productos químicos
- Plantas nucleares civiles
- Comunicaciones
- Defensa
- Servicios de emergencia
- Energía
- Finanzas
- Alimentación
- Gobierno
- Sanidad
- Espacio

- Transporte
- Agua

Varios sectores tienen "subsectores" definidos. Los servicios de emergencia, por ejemplo, pueden dividirse en policía, ambulancias, bomberos y guardacostas.

La Oficina del Gabinete del Reino Unido solía publicar Resúmenes del sector de seguridad y planes de resiliencia, el último de los cuales estuvo disponible en 2018. De esta publicación dos páginas resultan de interés: la página 14 sobre servicios de emergencia y la 12 sobre comunicaciones.

5. Estados Unidos

La Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) es la entidad líder operativa de la seguridad a nivel federal y coordinadora a nivel nacional en materia de seguridad y resiliencia de las infraestructuras críticas. En el siguiente enlace puede encontrarse más información sobre su papel en el sector de las comunicaciones: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/communications-sector

El sector de las comunicaciones está estrechamente vinculado a otros sectores, entre ellos los siguientes:

- El sector de la energía, que suministra energía para el funcionamiento de torres de telefonía celular, oficinas centrales y otras instalaciones de comunicaciones críticas y depende de las comunicaciones para ayudar en el monitoreo y control del suministro de electricidad.
- El sector de la tecnología de la información, que proporciona sistemas y servicios de control críticos, arquitectura física e infraestructura de Internet, y depende de las comunicaciones para distribuir aplicaciones y servicios.
- El sector de servicios financieros, que depende de las comunicaciones para la transmisión de transacciones y operaciones de los mercados financieros.
- El sector de los servicios de emergencia, que depende de las comunicaciones para dirigir los recursos, coordinar la respuesta, operar los sistemas de alerta y advertencia al público y recibir llamadas de emergencia en el número 911.
- El sector de sistemas de transporte, que se encarga de distribuir el combustible diésel necesario para alimentar los generadores de reserva y depende de las comunicaciones para monitorear y controlar el flujo de tráfico terrestre, marítimo y aéreo.

La misión del sector de servicios de emergencia es salvar vidas, proteger propiedades y el medio ambiente, asistir a las comunidades afectadas por desastres y ayudar a la recuperación durante las emergencias. En el siguiente enlace se encontrará más información sobre el papel de CISA en este sector: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/emergency-services-sector

Cinco disciplinas distintas componen el sector de servicios de emergencia, que abarcan una amplia gama de funciones y papeles de respuesta a emergencias:

- Orden público

- Servicios de extinción de incendios y salvamento
- Servicios de urgencias médicas
- Gestión de emergencias
- Obras públicas

El sector de servicios de emergencia también presta servicios especializados de manera individual y en equipos. Estas capacidades especializadas pueden encontrarse en una o varias disciplinas distintas, dependiendo de la jurisdicción:

- Equipos tácticos (por ejemplo, SWAT)
- Equipos de artefactos peligrosos/desactivación de bombas y seguridad pública
- Equipos de buceo/unidades marítimas
- Unidades caninas
- Unidades de aviación (es decir, helicópteros policiales y de evacuación médica)
- Materiales peligrosos (es decir, HAZMAT)
- Equipos de búsqueda y rescate
- Centros de respuesta de seguridad pública (es decir, centros de llamadas 911)
- Centros mixtos
- Equipos de seguridad privada
- Apoyo civil de la Guardia Nacional

El sector de servicios de emergencia de Estados Unidos es una comunidad integrada por millones de personas debidamente capacitadas, que cuentan con los recursos físicos y cibernéticos que les permiten prestar una amplia gama de servicios de prevención, preparación, respuesta y recuperación, tanto en operaciones estacionarias como de gestión de incidentes. En este sector se incluyen instalaciones y equipos que están distribuidos a lo largo de todo el país, además del personal altamente calificado que presta servicios tanto de manera remunerada como voluntaria. Este sector está organizado principalmente en los niveles de Gobierno federal, estatal, local, tribal y territorial y cuenta con departamentos de policía en las ciudades, oficinas del sheriff en condados, departamentos de policía y bomberos, departamentos de defensa y de obras públicas en las ciudades. Incluye también recursos del sector privado, como cuerpos de bomberos industriales, empresas de seguridad privada y proveedores privados de servicios médicos de urgencia.

Dado que el sector de servicios de emergencia se centra en la protección de otros sectores y el público en general, surgen retos únicos a la hora de abordar la seguridad y la resiliencia del propio sector como infraestructura crítica. Si alguno de los activos, redes o sistemas de este sector, ya sean físicos o virtuales, llegaran a quedar incapacitados, podría haber importantes daños o pérdidas de vidas humanas, problemas de salud pública o pérdidas económicas de largo plazo.

Este sector está formado por sistemas y redes integrados por componentes físicos, cibernéticos y humanos.

6. América Latina

Se utilizan los ejemplos de Ecuador y Costa Rica para dar una idea del panorama en América Latina.

Ecuador

Definición de infraestructura crítica. Según la Política Nacional de Ciberseguridad de Ecuador, emitida por el Ministerio de Telecomunicaciones, para lograr un ciberespacio digital seguro que garantice el Estado de derecho, proteja los servicios e infraestructuras críticas del Estado y brinde seguridad a la población en el ciberespacio, el Gobierno trazó un plan de acción basado en siete pilares:

- Gobernanza de ciberseguridad
- Sistemas de información y gestión de incidentes
- Protección de servicios e infraestructuras críticas digitales
- Soberanía y defensa
- Seguridad pública y ciudadana
- Diplomacia en el ciberespacio y cooperación internacional
- Cultura y educación de ciberseguridad

Las acciones contempladas en estos pilares buscan privilegiar el fortalecimiento institucional y la articulación efectiva de múltiples actores por parte del Gobierno. Las entidades gubernamentales y privadas del país deben cooperar con responsabilidad para lograr un ciberespacio digital seguro. El vínculo entre ciberseguridad e infraestructuras críticas queda definido en la Estrategia Nacional de Ciberseguridad, que debe contar con el apoyo de cada Gobierno y lograr resultados.

La Ley de Seguridad Pública y del Estado contempla la protección de las infraestructuras críticas en la estrategia nacional sobre la materia que elaboró el Ministerio de Telecomunicaciones.

Las principales entidades responsables de infraestructuras críticas, ciberseguridad y respuesta a emergencias son los ministerios de Telecomunicaciones y de Defensa, así como el servicio integrado de seguridad ECU 911.

Existe también el Consejo de Seguridad Pública y del Estado, el cual está integrado por el presidente, el vicepresidente, el presidente de la Asamblea Nacional, el presidente de la Suprema Corte de Justicia, los ministros de Seguridad, de Defensa Nacional, del Interior, de Asuntos Exteriores, el Jefe del Mando Conjunto de las Fuerzas Armadas y el Comandante General de la Policía Nacional.

Costa Rica

La Oficina de las Naciones Unidas para la Reducción del Riesgo de Desastres (UNDRR) señala que las infraestructuras críticas de Costa Rica incluyen los sectores acordados con la Comisión Nacional de Prevención de Riesgos y Atención de Emergencias (CNE). Esos sectores son los siguientes: (i) electricidad, (ii) petróleo, (iii) carreteras y puentes, (iv) ferrocarriles, (v) agua y saneamiento, (vi) salud, (vii) educación y (viii) correos.

Se considera que estos sectores son fundamentales para el funcionamiento y la resiliencia del país y que abarcan desde servicios esenciales como la salud y la educación hasta infraestructuras clave como la energía, el transporte y las comunicaciones. La protección de estos sectores es crucial para garantizar la seguridad, el bienestar y el desarrollo sostenible de Costa Rica.

Se puede encontrar más información en Qualitive assessment of critical infrastructure in Costa Rica | UNDRR

El vínculo entre la ciberseguridad y las infraestructuras críticas en Costa Rica se ha visto reforzado significativamente gracias a la Estrategia Nacional de Ciberseguridad 2023-2027. En esa estrategia se reconoce la importancia de proteger los sistemas digitales y la infraestructura tecnológica que sustentan los servicios esenciales del país. Se centra en reforzar la gobernanza de la ciberseguridad y mejorar la protección de las infraestructuras y la resiliencia cibernética a nivel nacional. La protección de las infraestructuras críticas es uno de los principales retos identificados, incluida la ciberdefensa, y el refuerzo de las normas, organizaciones y tecnologías relacionadas con la ciberseguridad.

Este enfoque integrado pone de manifiesto la interdependencia entre la seguridad física y la ciberseguridad, poniendo de relieve la forma en que la protección de activos críticos abarca no solo medidas físicas, sino también la defensa contra las amenazas digitales. Al proteger las infraestructuras críticas de ataques cibernéticos, Costa Rica pretende garantizar la continuidad y la fiabilidad de servicios esenciales como la energía, la atención de la salud, el agua y el transporte, que son fundamentales para la seguridad nacional y el bienestar de los ciudadanos. Si bien no existe una ley específica sobre infraestructuras críticas, hoy día se está tramitando un proyecto de ley sobre ciberseguridad en el que están incluidas.

Además, el Plan Estratégico Nacional para 2050, que no se centra exclusivamente en las infraestructuras críticas, contempla mejoras en las infraestructuras para la conectividad y la transición a una economía baja en emisiones de carbono, digital y descentralizada, lo que también contribuye a la seguridad nacional a largo plazo.

Este enfoque integrado es símbolo de que Costa Rica reconoce la necesidad de una estrategia holística de seguridad nacional que incluya la protección y el reforzamiento de las infraestructuras críticas, considerando tanto las amenazas físicas como las digitales, para garantizar la continuidad y la eficiencia de los servicios esenciales y la seguridad del país en general.

En Costa Rica, las principales entidades gubernamentales responsables de las infraestructuras críticas, la ciberseguridad y la gestión de emergencias son las siguientes:

- Comisión Nacional de Prevención de Riesgos y Atención de Emergencias (CNE)
- Equipo de Respuesta a Incidentes de Seguridad Informática del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones
- Ministerio de Seguridad Pública
- Instituto Costarricense de Electricidad (ICE)
- Ministerio de Salud
- Caja Costarricense de Seguro Social (CCSS)